Gizakiekin egindako ikerketetan datuak babesteari buruzko gida

Guía de protección de datos en investigación con seres humanos

A Guide to Data Protection in Human Research



IIEB CEID Koadernoak

IIEB CEID Cuadernos

IIEB CEID Notebooks

IKERKETA
ERRETOREORDETZA

VICERRECTORADO
DE INVESTIGACIÓN

eman ta zabal zazu

Universidad
del País Vasco

Euskal Herriko
Unibertsitatea

Gizakiekin egindako ikerketetan datuak babesteari buruzko gida

---

Guía de protección de datos en investigación con seres humanos

---

A Guide to Data Protection in Human Research

Gizakiekin egindako ikerketetan datuak babesteari buruzko gida

---

Guía de protección de datos en investigación con seres humanos

---

A Guide to Data Protection in Human Research

CEID - UPV/EHU

2020

Mabel Marijuán (CEID UPV/EHU)
M.ª Jesús Marcos (CEID UPV/EHU)

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

Leioa (ekaina / junio / June - 2020)

Cuadernos CEID

Vicerrectorado de Investigación

Revisores: Andoni Juaristi (DPD UPV/EHU), Alejandro Artetxe (DPD Hermanas Hospitalarias Provincia de España), Pablo Hernando (DPD Consorcio Hospitalario Parc Taulí), Pilar Nicolás (CEISH UPV/EHU)

Traducción inglesa: Aliuska Duardo Sánchez.
Financiada por el Proyecto de Investigación PANELFIT (EU Commission, H2020 SWAFS Programme, PANELFIT Project, research Grant Number 788039)

ceid@ehu.eus

Depósito legal/Lege gordailua: BI-1649-2020

Gizakiekin egindako ikerketetan datuak babesteari buruzko gida

Arau hauetan oinarrituta: Datuak Babesteari buruzko Europako Erregelamendua (DBEO) eta Datu pertsonalak babesteari eta eskubide digitalak bermatzeari buruzko 3/2018 Lege Organikoa (DPBL-EDB)

Aurkibidea

Aurkezpena

Datu pertsonalen babesak pertsonen askatasuna eta bizitza pribatua babesteko borondateari erantzuten dio. Zeregin etikoki baliotsua da, lege zehatzetan jaso dena, eta hori gogoan izan behar dugu beti, erantzukizunez jarduteko eta ez bakarrik legea bete behar delako. Sineste sendo hori barneratzen dugunean errazagoa da datuak babesteari buruzko zalantzak eta egoera zehatzak argitzea, baita, horrenbestez, pertsonen pribatutasuna eta autonomia egoki zaintzea ere.

DATU PERTSONALEN ERABILERA IKERKETAN: Ikertzen duzuenon erantzukizuna da ikerketaren subjektu izatea onartu duten pertsonak babestea, bai datu pertsonalen erabilera eskatzen duten ikerketetan, bai giza lagin biologikoak behar dituzten edo boluntarioen parte hartze zuzena eskatzen duten ikerketan.

Eskuliburu labur honen bidez, gure ikerketetan erabiliko ditugun datuen iturri edo emaileak diren subjektuei zor diegun zaintza erraztu nahi dizuegu, eta aintzat hartu dugu bai oinarrizko ikerketa, bai ikerketa aplikatua edo tutoretzapekoa, hala nola doktorego tesiak, master amaierako lanak eta gradu amaierako lanak. Parte hartzaileei edo emaileei zor diegun zaintza hori haien intimitatearen, pribatutasunaren eta askatasunaren babesean gauzatzen da, konfidentzialtasuna eta indarreko legezkotasuna betetzea sustatuz.

Proiektu bat diseinatzean galdera horiei erantzun behar diezue, zuen ikerketa jarduera abian jarri baino lehen, baldin eta pertsonen datuak beharko badituzue.

Zure ikerketa proiektua antolatzeko oinarrizko 20 galdera

1. Zein da zure ikerketa jardueraren izena?
2. Hori egiteko pertsona batzuek informazioa eman behar dizute?
3. Zer datu zehatz behar dituzu?
4. Ikuspegi metodologikotik, zertarako behar dituzu datu horiek?
5. Datuak pertsonengandik eskuratuko dituzu zuzenean?
6. Zer bitartekoren bidez (inkesta, elkarrizketa, historia klinikoa) atera eta bilduko dituzu datuak?
7. Behar adina informazio zehatza eta sinesgarria duen dokumentu bat prestatu duzu emaileei zer eskatuko diezun eta informazio hori zertarako erabiliko duzun azaltzeko?
8. Dokumentuan emaileen eskubideei eta haiek erabiltzeko aukerari buruzko informazioa sartu duzu?
9. Emaileak ez diren beste iturri batzuetatik datuak ematen badizkizute, nola egingo dute?
10. Datuak eskuratzen dituzunean, identifikazio pertsonala saiheste aldera, *seudonimiazatuko* dituzu, datuak eta identitateak kodeekin bereizita?
11. Non gordeko dituzu datuak eta non landuko dituzu ikerketak iraun bitartean?
12. Nork eskuratuko eta erabiliko dituzte datuak ikerlana egiteko?
13. Zenbat denbora beharko duzu datu horiek lantzeko eta gero gordetzeko?
14. Aurreikusita duzu zure ikertaldekoak ez diren pertsonei datuak uztea?
15. Beren datuak eman dizkizuten pertsonei zer kalte egin diezaieke zuri datuak galtzeak edo norbaitek legez kanpo erabiltzeak?
16. Zer kalte egin diezaioke ikerketari jasotako datuak eskuratzeko aukera ez izateak?
17. Zer bitarteko aurreikusi dituzu datuen legez kontrako erabilera saihesteko? Eta datuak ez galtzeko? Eta datuak eskuratzeko aukera ez blokeatzeko?
18. Pertsonen datu horiek erabiltzeak sortutako babes betebehar horiek zure taldeko kide guztiei transmititzeko protokolo, dokumentu edo tutorialen bat egin duzu?
19. Prestatua duzu dokumenturen bat zure ikerketarako jasotako informazioa babesteko egiten ari zaren guztia erregistratzeko?
20. Jarri zara harremanetan zure erakundeko datuen babeserako ordezkariarekin (DBO) datuen babesari lotutako alderdi guztien gainean pentsatzen eta lana ongi egiten lagun diezazun?

Galdera horien erantzunak, araudien eskakizunen arabera, zazpi urrats hauetan laburbildu daitezke:

1. **Identifikatu oinarrizko hamar alderdi:** (1) datu pertsonalak diren, (2) zertarako erabiliko dituzun, (3) zein da haien jatorria, (4) interesdunak (errekrutatuak/emaileak), (5) datu bereziak diren, (6) zer tratamendu egingo dituzun, (7) zer pertsona arduratzen diren horretaz, (8) hirugarrenei uzteko aukerak, eta (9) nazioartera transferitzeko aukerak. (10) jar zaitez harremanetan DBOrekin.

2. **Jardun zilegitasunez,** ikerketan erabilitako datu pertsonalen *tratamendu legitimo*[1] baterako baldintzak beteta, bereziki datu bereziak badira. Ikerketetan, eskuarki datu emaileen Adostasun Informatua izaten da tratamenduaren legitimazioa, baina, salbuespen gisa, beste legitimazio iturri batzuk ere egon daitezke.

3. **Informatu,** interesdunari; hots, datuak eman dituenari beharrezkoa den informazio guztia emanez, haren *eskubideak*[2] erabiltzeko aukera barne.

4. **Jaso ezazu interesdunen adostasun esplizitua**[3]**.**

5. **Hartu zure gain** datuak eskatu diezun pertsonen gaineko **ardura:** jar zaitez harremanetan zure ikastegiko DBOrekin, haren laguntzaz datu pertsonalen *tratamenduaren arriskuak analizatzeko* eta, hala behar bada, *eragin ebaluazio bat* egiteko.

6. **Bermatu segurtasuna,** *segurtasun neurri* teknikoak eta *antolakuntzako neurri* egokiak aplikatuta, hautemandako arriskuak kontuan hartuta. Horren guztiaren inguruan aholkularitza emango dizu ikastegiko DBOak.

---

[1] Datuak biltzea, gordetzea, erabiltzea, kontserbatzea, baita uztea ere.

[2] SZEATM eskubideak.

[3] **Esplizitua:** subjektu emaileak berariazko adostasun adierazpen bat igortzen du (baieztapen ekintza argi bat), adibidez, Dokumentu bat sinatzea, edo «Onartzea» sakatzea ingurune elektroniko batean.

7. **Dokumentatu diligentziaz** zure ikastegiko datuen babeserako ordezkariaren (DBO) laguntzaz, zure tratamendua UPV/EHUren edo ikertzen duzun ikastegiaren tratamendu jardueren erregistroan inskribatzeko (1), sinatutako adostasunak nola gorde zehazteko (2), interesdunaren eskubideen erabilera dokumentatzeko harekin koordinatuta (3), arriskuak analizatzeko eta, hala behar bada, eragin ebaluazioa egiteko (4), gorabeherak kudeatzeko (5), sinatutako konfidentzialtasun konpromisoak biltzeko (6), eta, hala behar bada, tratamendu eragileen kontratuak biltzeko (7).

Gizakiekin egindako ikerketetan datuak babesteko zazpi urratsak

1. URRATSA. Identifikatu oinarrizko hamar alderdi:

1. Datu pertsonalak diren.
2. Zertarako erabili nahi dituzun.
3. Non eta nola jasoko dituzun.
4. Interesdunak, errekrutatuak edo emaileak.
5. Datu bereziak diren.
6. Egin beharreko tratamenduak: artxibatzea, ordenatzea, analizatzea, gordetzea, etab.
7. Proiektuaren alderdi horren arduradunak: zer erakundetan ikertzen duzun, IN edo haren ordezkoa.
8. Hirugarrenei uzteko aukerak.
9. Nazioartean transferitzeko aukerak.
10. JAR ZAITEZ HARREMANETAN DATUEN BABESERAKO ORDEZKARIAREKIN.

2. URRATSA. Jardun zilegitasunez. Tratamendua legitimoa izan dadila.

3. URRATSA. Informatu. Eman datuak utzi dituenari beharrezkoa den informazio guztia, eskubideak* erabiltzeko aukera barne.

4. URRATSA. Eskatu adostasun esplizitua datuak eman dizkizuten pertsonei.

5. URRATSA. Hartu zure gain datuak eskatu diezun pertsonen gaineko **erantzukizuna**: jar zaitez harremanetan zure ikastegiko DBOrekin, haren laguntzaz datu pertsonalen tratamenduaren arriskuak analizatzeko eta, hala behar bada, eragin ebaluazio bat egiteko.

6. URRATSA. Bermatu segurtasuna. Aplikatu horretarako segurtasun neurri teknikoak eta antolakuntza neurri egokiak, hautemandako arriskuak kontuan hartuta eta zure DBOren aholkularitza jasota.

7. URRATSA. Dokumentatu zure DBOren laguntzaz:

1. Inskribatu zure tratamendua ikertzen duzun ikastegiaren jardueren erregistroan.
2. Zehaztu nola gorde emaileek sinatutako adostasunak.
3. Utzi prestatuta SZEATM eskubideak erabiltzeko bitartekoa.
4. Egin zure DBOrekin batera arriskuen analisi on bat eta, hala behar bada, eragin ebaluazio bat.
5. Aurreikusi balizko gorabeheren kudeaketa.
6. Jaso sinatutako konfidentzialtasun konpromisoak.
7. Jaso tratamenduaren arduradunen kontratuak (halakorik bada.

1. Identifikatu

Gogoeta egin eta proiektatu: (1) datu pertsonalak diren, (2) zertarako erabiliko dituzun, (3) zein da haien jatorria, (4) interesdunak (errekrutatuak/emaileak), (5) datu bereziak diren, (6) zer trataera egingo dituzun, (7) zer pertsona arduratzen diren hortaz, (8) hirugarrenei uzteko aukerak, (9) nazioartera transferitzeko aukerak. (10) jar zaitez harremanetan zure ikastegiko DBOrekin.

Datu pertsonalak

Datu pertsonala identifikatutako edo identifika daitezkeen pertsona fisikoen gaineko edozein *informazio* mota da (zenbakizkoa, alfabetikoa, grafikoa, fotografikoa, akustikoa edo bestelakoa). Norbait identifikagarri izateko informazioak, nortasun fisikoari, fisiologikoari, ekonomikoari, kulturalari, hezkuntzakoari, erlijiosoari eta abarri buruzkoak, informazioaren jatorrian dagoen pertsona nor den jakitea ahalbidetzen dutenak.

Datu pertsonala: identifikatutako edo identifika daitezkeen pertsona fisikoen gaineko edozein informazio (zenbakizkoa, alfabetikoa, grafikoa, fotografikoa, akustikoa edo bestelakoa).

Helburua eta jatorria

Oso argi eduki behar duzu etorkizuneko ikerketa bat diseinatzean *zergatik eta zertarako* jasotzen, erregistratzen, aztertzen, gordetzen… dituzun datuak, baita datu horiek ezingo dituzula gero tratatu helburu horiekin bat ez datozen zereginetan ere; izan ere, datu pertsonalak helburu zehatz, esplizitu eta legitimoekin tratatu behar dira beti.

Kontuan hartu behar duzu, halaber, *datuen minimizatze irizpidea edo printzipioa*: soil-soilik ikerketa egiteko ezinbestekoak diren datuak jaso behar dituzu; ez jaso proiektuaren hasierako diseinuan aurreikusi gabeko datuak «agian aurrerago beharko dituzulako».

Jakina, zure proiektuan aurreikusi eta jasota utzi behar duzu ere informazio hori nondik eskuratuko duzun (emailetik zuzenean, historia klinikoko dokumentuak, txotenak edo zeharkako beste iturri batzuk).

HELBURUEI ETA JATORRIEI BURUZKO 5 Wak

WHAT/zer: Deskribatu zehaztasunez jaso behar duzun informazioa edo datu mota. *Datuak minimizatzeko printzipioa: soilik ezinbesteko datuak jasotzen dira.*

WHY/zergatik: Azaldu argi zertarako nahi dituzun bildu, erregistratu, aztertu, analizatu, gurutzatu, kontserbatu, etab.

Helburuaren mugak: gero ezingo dituzu tratatu helburu horiekin bateragarria ez den modu batean.

WHERE/non: Zehaztu nondik jasotzen dituzun; hau da, emailetik zuzenean, historia klinikotik, espedienteetatik edo zeharkako beste iturri batzuetatik, eta adierazi nola jaso dituzun (elkarrizketak, inkestak, testak, fitxak, etab.). *Konfidentzialtasuna.*

WHO/nor: Jaso emaile izango diren boluntarioen profila eta adierazi nork egingo duzuen tratamendua. *Adostasun informatua.*

WHEN/noiz: Ordenatu urrats bakoitzaren denborak: biltzea, *seudonimizazioa* egitea, gordetzea, transferentzia, etab.

Interesdunen kategoria

Legediak «interesdun» deitzen die informazio propioa ematen duten pertsonei; informazio bat, gero zure ikerketarako datutan eraldatuko duzuna.

Egia esateko, ikerketarako *erreklutatutako pertsonak* edo *emaileak* dira; hau da, datuak zertarako behar dituzun, nola erabiliko dituzun eta nola babestuko dituzun azaldu ondoren, eskatutako informazioa ematen dizuten pertsonak.

Datuen kategoria bereziak

Datu batzuk, zure ikerketarako beharrezkoak izan daitezkeenak, kontu handiagoz eta baldintza jakin batzuk beteta zaindu behar dituzu, emaileen pribatutasunerako daukaten garrantzia dela eta.

Datu pertsonal guztiak ez dira berdinak, eta araudiak honela sailkatzen ditu:

Datu sentikorrak edo bereziki babestuak

Datuen kategoria bat da, *eragin berezia dutelako emailearen intimitatean, askatasun publikoan eta oinarrizko eskubideetan.* Hori dela eta, gainerako datu pertsonalei baino babes handiagoa eskaini behar diezu (DBEO, 9. artikulua eta 51-56 kontsideratuak):

- Ideologia edo iritzi politikoak.
- Sindikatu afiliazioa.
- Erlijioa edo iritzi erlijiosoak.
- Sinesmenak edo sinesmen filosofikoak.
- Arraza edo etnia jatorria.
- Osasunari buruzko datuak[1].
- Bizitza sexuala edo orientazio sexuala.
- Genero indarkeria eta tratu txarrak.

- Datu genetikoak[2].
- Datu biometrikoak[3].
- Zigorrei eta zigor delituei buruzko datuak.
- Zehapen administratiboei buruzko datuak.

Unibertsitateko eta beste zentro batzuetako ikerketa jardueretan ohikoa izaten da datu sentikor mota guztiak erabiltzea, askotariko arlotan ikertzen delako, hala nola zientzia biologikoak, teknikoak, sozialak, juridikoak eta portaerari buruzkoak. Alabaina, bereziki delikatuak dira:

[1] **Osasunari buruzko datuak.** Pertsona baten osasun fisikoaren edo mentalaren egoerari buruzko informazioa ematen duten datu guztiak, osasun arretako zerbitzuen prestazioa barne hartuta. Izan ere, gaixotasunei, desgaitasunei, gaixotasunak izateko arriskuei, tratamendu klinikoei, egoera fisiologiko edo biomedikoari… buruzko informazioak osasun datuak dira, alde batera utzita haien iturria den historia klinikoa, mediku bat edo osasun arloko beste profesional bat, ospitale bat, gailu mediko bat, *in vitro* proba diagnostiko bat, edo jardueran parte hartzen duen pertsonak berak emandako informazio bat.

Kontuan hartu behar duzu beti informazio hori biltzeko, erabiltzeko, gordetzeko… datuak babesteko araudia, beste askoren artean, *Pazientaren Autonomiari buruzko 41/2002 Legearekin* osatzen dela, zeinak informazio eta dokumentazio klinikoaren arloko eskubideak eta betebeharrak arautzen baititu, barne hartuta komunikazioa, erabakiak hartzea, adostasun informatua, historia klinikoa eskuratzea, etab.

[2] **Datu genetikoak.** Osasun datu espezifikoak dira; azido nukleikoen analisiaren bidez edo bestelako analisi zientifikoen bidez lortzen dira, eta pertsonen ezaugarri hereditarioei buruzko informazioa identifikatzen dute.

[3] **Datu biometrikoak.** Pertsona baten ezaugarri fisikoei eta fisiologikoei edo portaerari buruzko informazioak dira; teknika espezifikoen bidez lortzen dira (adibidez, aurpegiaren irudiak, datu daktiloskopikoak, etab.), eta pertsona baten identifikazio bakarra ahalbidetzen edo baieztatzen dute (DBEO, 4.14 artikulua).

Adingabeen datuak

Hasiera batean ez dira datu sentikorrak, baina araudian adierazten da *adingabeen kalteberatasuna* dela eta halakotzat tratatu behar dituzula; izan ere, pertsona horiek ez dira guztiz jabetzen beren datuak jasotzeari eta erabiltzeari lotutako arriskuez, ondorioez, bermeez eta eskubideez, eta zure erantzukizuna da haien datuak urratuak izan ez daitezen.

Modu orientagarrian, kontuan hartu honako hau: baldin eta eskatuko dituzun datuek adingabeari tentsio edo afektazio larriren bat eragin badiezaiokete, zure ikerketa inbaditzailetzat hartuko da, eta, hortaz, baimena eskatu beharko diezu adingabearen lege ordezkariei (gurasoei edo tutoreei), eta ziurtatu beharko duzu 12 urtetik aurrera adingabeak berak baiezkoa ematen duela. Datuak horrelakoak ez direnean, 14 urtetik beherako adingabeen kasuan nahikoa izango duzu legezko ordezkarien baimena lortzea, adin horretatik aurrera haien esku baitago baimena ematea ala ez. Proiektua ebaluatzen duen DBOak eta etika batzordeak orienta diezazukete sortutako zalantzen inguruan, kasuistika askotarikoa baita eta legea ez baita hertsia gai horri dagokionez.

Ikerketa mota	Adina	Adostasuna
Ikerketa inbaditzailea datuekin	18 urtetik beherakoak	Legezko ordezkariek ematen dute adostasuna. 12 urtetik gorakoak baiesten du.
Ikerketa ez-inbaditzailea datuekin	14 urtetik beherakoak	Legezko ordezkariek ematen dute adostasuna. 12 urtetik gorakoak baiesten du.

Kalteberatasun egoera berezian dauden kolektiboetako pertsonen datuak

Arreta berezia jarri behar duzu ikerketa jarduerak kalteberatasun egoera berezian dauden kolektiboetako datuak erabiltzea eskatzen badu; horien artean daude, besteak beste, adingabeak (dagoeneko aipatu ditugunak), desgaituak, agureak, gizarte bazterkeria arriskuan dauden pertsonak, egoera politiko konprometituan dauden pertsonak, paperik gabekoak, etab.

DATU SENTIKORRAK EDO BEREZIKI BABESTUAK

Ideologia edo iritzi politikoak
Sindikatu afiliazioa
Erlijioa edo iritzi erlijiosoak
Sinesmenak edo sinesmen filosofikoak
Arraza edo etnia jatorria
Osasunari buruzko datuak
Bizi edo orientazio sexualak
Genero indarkeria eta tratu txarrak
Datu genetikoak
Datu biometrikoak
Zigorrei eta zigor delituei buruzko datuak
Zehapen administratiboei buruzko datuak

Nahikoa arrunta izaten da emailearen intimitatean, askatasun publikoetan eta oinarrizko eskubideetan eragin berezia duten datuak erabiltzea, askotariko arlotan ikertzen delako, hala nola zientzia biologikoak, teknikoak, sozialak, juridikoak eta portaerari buruzkoak.

Datuen tratamendua

«Datuen tratamendua» esaten zaio datu pertsonal batean, edo pertsonala izan gabe, haien multzokatzeak pertsona bat identifikatzen duenean, edo datuen multzo batean eraldatutako informazio pertsonalaren gainean egiten duzun edozein eragiketa edo eragiketa multzori, zeina prozedura automatizatuen bidez egin daitekeen, ala ez. Hala, datu tra-

tamendutzat hartzen da: datuak biltzea, erregistratzea, antolatzea, egituratzea, gordetzea, egokitzea edo aldatzea, ateratzea, kontsultatzea, erabiltzea, transmisio bidez komunikatzea, zabaltzea, edo haiek eskuratzeko, erkatzeko edo interkonektatzeko, mugatzeko, ezabatzeko edo suntsitzeko beste moduren bat egokitzea.

Ikerketa jarduera batean gerta daiteke datu pertsonalen tratamendu bat edo batzuk egin behar izatea. Izan ere, zure ikertaldeko kideei buruzko informazioa (datu pertsonalak) tratatu beharko dituzu beti eta, batzuetan, ikerketa aurrera eramateko behar dituzun datuen jabe diren pertsonen informazioa.

DATUEN TRATAMENDUA

Prozedura automatizatuen bidez edo ez, datuekin egindako eragiketa edo eragiketa multzo oro, hala nola:

- Biltzea.
- Erregistratzea.
- Antolatzea.
- Egituratzea.
- Gordetzea.
- Egokitzea.
- Aldatzea.
- Seudonimizatzea.
- Anonimizatzea.
- Ateratzea.
- Kontsultatzea.
- Erabiltzea.
- Transmititzea.
- Zabaltzea.
- Sartzeko egokitzea.
- Erkatzea.
- Interkonektatzea.
- Mugatzea.
- Ezereztea.
- Suntsitzea.
- Etab.

Datuen tratamenduaren adibideak dira, besteak beste: ikertzaileei buruzko informazioa kudeatzea (biltzea, artxibatzea eta erabiltzea), datuen tratamendu hori ikerketarako ez izan arren; parte hartzaileei eskatutako informazioa kudeatzea (biltzea, artxibatzea eta erabiltzea); seudonimizazioa; kodetzea edo bereiztea; adostasun informatuaren dokumentu idatziak gordetzea; etab.

Terminoa nahasgarria gerta dakizue; izan ere, ikerketa batean datuen tratamenduak esperimentuetatik eskuratutako datuetatik ondorioak ateratzeko erabilitako *estatistika edo analisi metodo* bati egin ohi dio erreferentzia, eta esperimentu horiek, eskuarki, laborategian, laginetan, landa lanetan edo jarduera zientifiko bakoitzaren berezko metodologia aplikatzen ari den beste esparru batean egiten dira.

Tratamenduaren arduraduna

Haren izenak dioen moduan, datuen tratamenduaz arduratzen den pertsona fisikoa edo juridikoa da, eta horrela identifikatuta egon behar du beti ikerketa orotan.

Esate baterako, tratamendu jardueren erregistroan (TJE) kontsignatutako tratamendu guztien arduraduna UPV/EHU da. Izan ere, **ikertzaile nagusia edo tesiaren, MALen edo GRALen tutorea edo zuzendaria tratamenduaren barne arduraduna da** ondorio praktikoetarako, baina unibertsitatean datu pertsonalekin egindako tratamendu guztien arduraduna UPV/EHU da beti.

Ikerketaren arduradun gisa, inoiz behar badituzu zure jarraibideen arabera datu pertsonalak tratatuko dituen pertsona edo enpresa baten zerbitzuak (esate baterako, zerbitzu informatikoen enpresa bat), nahitaezkoa da erakundeak, gure kasuan UPV/EHUk, *Tratamendu eragilearen kontratu bat* sinatzea pertsona fisiko edo juridiko horrekin.

Datuak uztea edo komunikatzea

Datu pertsonalak ikerketarekin zerikusirik ez duten hirugarrenei (interesdun, ikertzaile baimendu eta tratamenduaren arduradun EZ diren guztiak dira hirugarrenak) utzi behar badizkiezu nahitaezkoa da datuak eman dituen pertsonaren *berariazko adostasun idatzia* lortzea.

Kontuan hartu behar duzu egoera berezi hau ematen da: hirugarren pertsonei emango diezun informazioak ikerketa subjektutik edo emailetik ateratako datuak baditu eta datu horiek haren senideen informazio pertsonala eman badezakete, lagapena egiteko beharrezkoa izango da senide horien guztien berariazko adostasun idatzia edukitzea.

Nazioarteko datu transferentziak

Datuen nazioarteko transferentzia datu pertsonalak Europar Batasunetik kanpo transmititzean datza. Bai zu, ikertzaile gisa, bai ikertzeko duzun erakundea, tratamenduaren arduraduna dena, esportatzaileak izango zarete, Europako herrialde batean zaudetelako eta nazioarteko transferentzia bat egingo duzuelako.

Ikerketaren datu pertsonalak beste herrialde batera edo nazioarteko erakunde batera transferitu ahal izango dituzu bakar-bakarrik babes maila egoki bat bermatzen badute, DBEOren V. kapituluan ezarritako baldintzen arabera. Datuak EBik kanpoko herrialde edo lurralde batera, hirugarren herrialde horren sektore espezifiko batera, edo nazioarteko erakunde batera transferitu behar badira eta Europako Batzordeak han babes maila egokia bermatzen ez dela irizten badio, aipatutako kapituluan jasotako egoeraren bat edo batzuk eman beharko dira —kasuistika oso luzea da gida honetan sartzeko—, transferentzia hori baimendu dadin. Kontsultatu V. kapitulua edo, hobe oraindik, galdetu zure ikastegiko DBOri.

Ikerketaren datu pertsonalak «hodeian» *(Cloud Computing)* gorde behar badituzu garrantzitsua da kontuan hartzea zerbitzu horiek ematen dituzten enpresa asko Europar Batasunetik kanpo daudela eta ez dituztela berme juridiko egokiak eskaintzen. Horrelakoetan, gogoratu ezinbestekoa dela zure DBOri kontsultatzea, informazio hori lor dezan.

Datuen Babeserako Ordezkaria (DBO)

> Datuen Babeserako ordezkari gisa jardun denak datu pertsonalen trataeraren inguruan planteatzen zaizkion egoera guztiak konpontzeko gai izan behar du. Ez da, ez datuen tratamenduaren arduraduna, ez eragilea, halako zereginak bere gain hartzeak konpromisoan jarriko bailuke haren neutraltasuna; halere, oinarrizko zeregin bat betetzen du datu pertsonalen kategori bereziak lantzen diren erakundeetan. (Sánchez Ors, 2019)

Datuen Babeserako Ordezkaria (DBO) —*Data Protection Officer (DPO) ingelesez*— espezialista bat da datuen babesean, unibertsitate publikoek eta pribatuek eta beste erakunde batzuek nahitaez izendatu behar dutena. DBO horrek erakunde arduradunari (gure kasuan, UPV/EHU) eta tratamenduaren barne arduradunei (gure kasuan, IN edo ikertaldean izendatutako pertsona) datuen babesari buruzko informazioa, aholkularitza eta laguntza eman behar die, baita haiek gai horren inguruan egindako galdera guztiei erantzun ere.

DBOk datuen babesari lotutako gaietan lege betebeharrak betetzen direla ziurtatu behar du, eta zaintza eta kooperazio lanak egin behar ditu kontrol erakundeekin (Datuak Babesteko Espainiako Agentzia eta Datuak Babesteko Euskal Bulegoa).

Ikertzailea zaren neurrian, harremanetan jarri behar duzu pertsona horrekin zure ikerketan datu pertsonalen tratamenduari lotutako alderdi guztietarako; izan ere, haren zereginen artean, honako hauek daude:

1. Zu informatzea eta aholkatzea.
2. Laguntza eta ikuskaritza eskaini behar dizue arriskuaren analisian, inpaktu ebaluazioetan eta horiek ikerketa proiektuetan aplikatzean.
3. Zure ikerketetan aplikagarriak diren segurtasun neurriak kontrolatu, koordinatu eta egiaztatu behar ditu.

Gainera, DBO ikerketaren etikako batzordearen (IEB) kidea da beti, eta zure proiektuari buruzko informazioa emango du; beraz, zuk datu pertsonalekin egindako ikerlanek eta hark BDO gisa egindako lanak lotura zuzena eta etengabea dute, halabeharrez.

DATUEN BABESERAKO ORDEZKARIA (DBO)

Zuk datu pertsonalekin egindako ikerlanen eta hark DBO gisa egindako lanaren arteko harremana nahitaezkoa, zuzena eta etengabea da.

- Informatzen, prestatzen eta aholkatzen du.
- Arriskuaren analisian, eragin ebaluazioetan eta haien aplikazioan laguntzen du, eta horiek guztiak gainbegiratzen ditu.
- Segurtasun neurri aplikagarriak kontrolatzen, koordinatzen eta egiaztatzen ditu.
- Gorabeheren kudeaketa zaintzen du.
- Emaileentzako erreferente bat da, datuen babesari eta baliabideak erabiltzeari dagokionez.
- Erakundearen datuen babesari buruzko informazioaren eta dokumentazioaren antolakuntza ikuskatzen du.
- Ikerketako etika batzordeetako (IEB) kidea da. Batzorde horietan ikerketa proiektuen alderdi metodologiak, etikoak eta juridikoak aztertzen dira.
- Lotura egiten du datuak babesteko erkide eta estatuko agentziekin.

2. Jardun zilegitasunez

Horrek esan nahi du, besterik gabe, baldintzak bete behar dituzula zure ikerketan datuen tratamendua legitimoa izan dadin (ongi egina eta segurua legearen ikuspegitik).

Tratamenduaren zilegitasuna

Zure ikerketan datuak erabiltzea ahalbidetzen dizun «oinarri juridiko» gisa ere ezagutzen dena: Zer datu hartuko dituzun, nori hartuko dizkiozun eta nola erabiliko dituzun erabaki ondoren, hori egitea legitimoa izango da bakar-bakarrik emaileen *adostasun informatua* baduzu. Adostasun hori modu askean, espezifikoan, esplizituan eta unibokoan eman beharko dute, datuak erabiliko dituzun helburu guztietarako (art. 6.1,2).

Datuen tratamendurako beste oinarri juridiko batzuek, hala nola *legezko betebeharrak, interes publikoak edo botere publikoen erabilerak,* ez diote balioa kentzen zure informazio eta adostasun betebeharrari gizakiekin egindako ikerketen arloan, ezta hura ordezkatzen ere, bakar-bakarrik egoera batzuk islatzen dituzte non emaileak interes publiko bat dagoela badakien (DBLOren 8. art. eta DBEO 9. art.).

Datu sentikorren tratamendua legitimatzeko baldintza orokorrak eta eskakizunak

Oro har, datu horiek biltzea, erabiltzea edo gordetzea, hau da, aurreko atalean deskribatutako datu sentikor edo bereziki babestuen tratamendua debekatuta badago ere, datu sentikorrak zure ikerketarako erabil ditzakezu jarraian aipatutako baldintzetako bat edo batzuk betez gero:

- *Interesdun/emailearen baimen esplizitua* duzu *ikerketa jarduera espezifiko* baterako.
- Datuak beharrezkoak dira *artxibatze eta interes publikorako*, *ikerketa zientifiko edo historikorako edo helburu estatistikoetarako*, eta beste batzuek *seudonimizatu* dituzte.
- Interes publikoko arrazoiak daude *osasun publikoaren arloan*.

Eta baldintza hauek bete behar dituzu:

a) Eskuratu errekrutatutako pertsonen *berariazko adostasun* idatzia; bertan, datuak ematea onartzen dutela baieztatu, eta datuak zertarako erabiliko diren eta nola tratatuko diren adieraziko da.

b) Ziurtatu informazio horren kalitatea; hau da, zure ikerketarako *datu egokiak, benetakoak eta beharrezkoak direla* ziurtatu, horien beharra haztatuz. Hau da, baloratu ea jasoko dituzun datu guztiak benetan beharrezkoak diren zure ikerketa egiteko. Ikerketarako beharrezkoak ez badira, datu pertsonalak ez dira eskatu behar (datuen minimizazio irizpidea edo printzipioa).

c) Ziurtatu ere datuak ez direla jasotzen modu desleialean, iruzurtian edo ez-zilegian.

d) Ez ahaztu zure ikerketarako osasun datuak bilduz gero, emailearen osasunari lotuta eskuratzen duzun edozein informazio erabilgarria eman behar diozula.

e) Egin *proportzionaltasun irizpen* bat lortu nahi duzun helburu zientifikoaren eta erabiliko duzun bitartekoaren artean.

f) Zure ikerketarako interesdunaren (emailea) historia klinikotik ateratako osasun datuak behar izanez gero, jaso beti *informazio eta adostasun orri edo dokumentu bat* non honako hauek jasoko diren:

- Pazientea artatua izan den profesionalaren eta zentroaren izena.
- Eskaeraren helburuak.
- Kasu klinikoa argitaratzeko adostasun adierazpena, osasun arloko profesionalentzako argitalpenetan.
- Pazientearen izena.
- Nortasun agiriaren dokumentua edo pasaportea, eta haren sinadura, bere historia klinikoaren datuak txostenean deskribatutako baldintzetan erabiltzeko berariazko baimena ematen.

g) Ziurtatu datuak eskuratzeko aukera duten pertsonek *konfidentzialtasun konpromisoa* betetzen dutela, baita aldeak lotzen dituen harremana amaitu denean ere.

> Zigor Kodea, 199. artikulua: 1. Norbaitek, bere ogibide edo lanharremanen ondorioz, inoren sekretuak badakizki, eta horiek ezagutarazten baditu, orduan, horri urtebetetik hiru arteko espetxealdi-zigorra ezarriko zaio, bai eta sei hilabetetik hamabi arteko isuna ere.
>
> 2. Profesionalak, bere isil-gordezko edo erreserbazko betebeharra hautsi eta beste pertsona baten sekretuak zabaltzen baditu, orduan, horri urtebetetik lau arteko espetxealdi-zigorra ezarriko zaio eta hamabi hilabetetik hogeita lau arteko isuna, eta lanbide horretarako desgaikuntza berezia, bi urtetik sei artekoa.

Kasu honetan, beste batzuetan bezala, ikerketaren kasuistika eta legearen (ez baitzen egin ikerketan bakarrik pentsatuta) zehaztugabetasuna hain dira askotarikoak, non zure DBOak eta zure ikastegiko ikerketaren etika batzordeak emandako orientazioa ezinbestekoa izango baita. Haiek jakingo dute alderdi horiek guztiak zuhurtziaz eta modu praktiko batean baloratzen.

Erabilera legitimoaren egoera bereziak osasun ikerketetan

Osasunari lotutako ikerketetan, bereziki biomedikuntzan, datu pertsonalak legitimotasunez erabil ditzakegu bi egoera berezi hauetan:

1. Ikerketaren helburua edo arloa lotuta dagoenean interesdunak baimendu zuen helburu edo arloarekin; esate baterako, minbizi mota jakin baten ikerketa datuen tratamendurako baimena eman zuenean eta datu horiek ikerketa onkologiko orokor batean erabili nahi dituzunean. *Eraginpeko pertsonak informatu* behar dituzu, eta aldez aurretik *Ikerketaren Etika Batzordearen* aldeko txostena behar duzu.
2. Beste talde batek datuak *seudonimizatu* ditu, tratamendu horretarako erreklutatutako pertsonen baimenez. BDOk *konfidentzialtasun konpromisoa* ziurtatzen eta *berridentifikazioa* saihesten lagunduko dizu.

(Ikus Datu pertsonalak babesteari eta eskubide digitalak bermatzeari buruzko 3/2018 Lege Organikoaren (DPBL-EDB) hamaseigarren xedapen gehigarria.)

3. Informatu

Zure ikerketarako datuak eskatuko diozun pertsonari eman iezaiozu beharrezkoa den informazio guztia, bere eskubideak erabiltzeko aukera barne hartuta; erabili hizkuntza argia, erraza, zehatza, gardena, ulergarria eta erraz ulertzeko modukoa.

Nork informatu behar du, eta noiz

Emaileei bere datuen tratamenduaren inguruko alderdiei buruzko informazioa emateko betebeharra ikerketaren barne arduradunari dagokio (IN edo hark izendatutako pertsona), eta erakundearen izenean, hots, UPV/EHUren izenean informatu behar du.

Jakina, informazio guztia jarri behar duzu balizko emaileen esku, datuak bildu baino lehenago.

Informatzeko betebeharraren salbuespenak

Ez da beharrezkoa informatzea:

- Emaileak dagoeneko informazioa duenean.
- Informatzea *ezinezkoa* denean edo *neurriz gaindiko ahalegin bat* eskatzen duenean; alabaina, halakoetan neurri egokiak eta zehatzak hartu beharko dituzu haren eskubideak babesteko.

Nola informatu

Zuzen informatzeko, informazioa ongi egokitu behar duzu datuak biltzeko erabiliko duzun eredura eta haren ezaugarrietara, aldakorrak izango baitira, besteak beste, luzerari, espazioari, argitasunari eta informazioak lotzeko aukerari dagokienez:

- Inprimakiak paperean.
- Inprimakiak webgunean.
- Elkarrizketa telefonoz edo aurrez aurre.

Gogoratu datuen babesa diligentziaz betetzeak informatu izanaren ziurtagiria gordetzera derrigortzen zaituela; hori dela eta, gomendagarria da *lehen mailako edo geruzako informazioa* idatziz ematea *adostasun dokumentuan*, hura jaso izana sinatzeko, eta jarri dokumentu horretan bigarren geruzako informazioa edo informazio osoa eskuratzeko esteka. Hurrengo atalean azaltzen da zer den informazioa bi geruzetan ematea.

Oso garrantzitsua: askotan aldi berean eskatuko diozu zure ikerketa jardueran parte hartzeko (*ikerketan parte hartzeko adostasun informatuaren dokumentua* oinarri hartuta) eta datu jakin batzuk emateko (*ikerketa horretarako datuak jasotzeko, erabiltzeko eta kontserbatzeko adostasun informatuaren* dokumentua). Gerta daiteke ere adostasun informatua eskatu behar izatea ikerketa berari lotutako beste alderdi batzuetarako (esate baterako, laginak edo bestelakoak hartzeko adostasun informatua).

Hausnartu, imajinatu eta antolatu, ikuspegi orokor batez, zure ikerketarako behar duzun informazioa eta adostasunak jasotzeko modua, interesduna larrituta edo nahastuta gera ez dadin.

Informazio egoki baten ezaugarriak honako hauek dira: soiltasuna, argitasuna, zehaztasuna, gardentasuna, ulergarritasuna eta eskuratzeko erraztasuna.

Informazioa geruza edo mailatan aurkeztea

DBEDBLOk txertatu du geruza edo mailen araberako informazioaren kontzeptu hori, eta datuak eskatzen dizkiozun pertsonari informazioa aurkezteko moduari dagokio.

Lehen mailan honela informatzen duzu:

- era laburtuan
- unean bertan
- datuak biltzeko erabiliko duzun bitarteko berean.

Gero informazio osagarria bidal diezaiokezu *bigarren maila* batean:

- informazioak modu zehatzago batean emanez
- aurkezteko, ulertzeko eta, hala nahi baduzu, artxibatzeko egokien irizten diozun bitartekoa erabiliz.

Adibidea: ikerketan parte hartzeko Adostasun Informatua (AI) eskatzeko dokumentu batek, paperean, ikerketarako datuek emateko adostasun informatua ere barne hartuko duenak, informazioaren *lehen geruza* jasotzen du, eta dokumentu horretan bertan, paperean, esteka bat jarri behar duzu informazioaren bigarren geruza dagoen webgunera sartzeko (AI dokumentuari buruzko eranskina).

Informazioaren lehen geruza edo lehen maila

Emaileari ematen diozun informazioaren oinarrizko edukia «lehen geruzari» edo «informazioaren lehen mailari» dagokio arauan, eta hori da, hain zuzen, balizko emaileek jakin behar dutena, zuri datuak ematea *onartzen duten ala ez* erabakitzeko.

1. Tratamenduaren kodea (Tratamendu Jardueren Erregistroan —TJE— ageri den kodea).
2. Tratamenduaren izena.

3. Tratamenduaren arduraduna (Erakundea: UPV/EHU, gure kasuan).
4. Datuen jatorria, emailetik ez datozenean.
5. Datuen tratamenduaren helburua.
6. Datuen tratamenduaren legitimazioa.
7. Datuen lagapenen hartzaileak eta nazioarteko transferentziak.
8. Eskubideak (sartzea, zuzentzea, ezereztea, aurkaratzea, transmititzea eta mugatzea —SZEATM—).

Informazio hori Datuen Babeserako ordezkariak emango dizu, zure tratamendua TJEn erregistratzen duenean.

Bigarren informazio maila edo geruza

Bigarren zehaztasun mailan informazio hau sartuko duzu:

1. Tratamenduaren kodea (Tratamendu Jardueren Erregistroan —TJE— ageri den kodea).
2. Tratamenduaren izena.
3. Tratamenduaren arduraduna: UPV/EHUren eta Datuen Babeserako ordezkariaren harremanetarako datuak.
4. Datuen jatorria, emailetik ez datozenean (zabaldua).
5. Datuen tratamenduaren helburua.
6. Datuak gordetzeko epea.
7. Datuen tratamenduaren legitimazioa.
8. Datuen lagapenen hartzaileak eta nazioarteko transferentziak.
9. Tratamenduaren datu pertsonalak (ikerketan tratatuko diren datuen zerrenda xehea).

10. Eskubideak eta horiek baliatzeko modua (sartzea, zuzentzea, ezereztea, aurkaratzea, transmititzea eta mugatzea —SZEATM—).
11. Informazio osagarria (UPV/EHUren datu pertsonalen babesari buruzko webgunerako esteka).

Informazio hori Datuen Babeserako ordezkariak emango dizu, zure tratamendua TJEn erregistratzen duenean.

DATUAK ESKATZEN DIZKIOZUN PERTSONARENTZAKO INFORMAZIOA

Edukia

- Benetakoa eta nahikoa luzea, zehatza, argia eta ulergarria.
- *Lehen mailako edo geruzako informazio* guztia adostasun dokumentuan idatziz ematea gomendatzen da.
- Jarri beti informazio osora edo bigarren geruzara sartzeko esteka bat.

Forma

- Egokitu informazioa datuak biltzeko eredura:
  - — Inprimakiak paperean.
  - — Inprimakiak webgunean.
  - — Elkarrizketa telefonoz edo aurrez aurre.
- Sartu adostasun dokumentu berean, ahal bada, parte hartzea eskatzen duzun ikerketari eta horretarako behar dituzun datuei buruzko informazioa, eta bientzako adostasun eskaerak.

Gordetzea

- Gorde, euskarririk egokienean, informatu eta adostasuna eskuratu izanaren ziurtagiria.

Informazioa emateko moduari buruzko UPV/EHUko GIEBren gomendioa (Gizakiekin eginiko Ikerketarako Etika Batzordea)

Oinarrizko informazioa aurkeztea (lehen geruza) eta UPV/EHUren TJE publikoan dagoen informazio osora (bigarren geruza) igortzea lege aukera bat da. Edonola ere, UPV/EHUko GIEBek adostasun informatuaren dokumentuan hurrengo klausula jartzea gomendatzen du —ikerketa bakoitzera behar bezala egokituta— epigrafe baten azpian, non idatzita egongo baita *Datuen babesari buruzko informazioa:*

- Datuen Babeserako Europako Erregelamenduaren (EU2016/679) arabera, informazio hau ematen zaizu:
- Datuen tratamenduaren kodea da: . . . . . .
- Datuen tratamenduaren izena da: . . . . . .
- Tratamenduaren helburua da: . . . . . .
- Datuen tratamenduaren arduraduna UPV/EHU da:

Identitatea: Universidad del País Vasco/Euskal Herriko Unibertsitatea

IFK: Q4818001B

Posta helbidea: Sarriena auzoa, z/g, 48940-Leioa (Bizkaia)

Webgunea: www.ehu.eus

Datuen Babeserako Ordezkariaren harremanetarako datuak: dpd@ehu.eus

- Eskatutako datu pertsonalak hauek dira: . . . . . .
- Zure datuak gordetzeko epea izango da: datuak gordeta edukiko dira interesdunak horiek ezerezteko eskatzen ez duen bitartean eta, edonola ere, errekurritzeko edo erreklamatzeko epeak irekita dauden bitartean edo eskuratu ziren helburuetarako baliagarriak diren bitartean.
- Tratamenduaren legitimazioa da: haren adostasun informatua (edo beste legitimazio iturri batzuk, hala behar bada).

- Lagapenak: (Adierazi lagapenak, edo, ez badira, idatzi hau: «Ez dira datuak utziko, non eta ez dagoen legezko aurreikuspenik»).
- Zure datuen nazioarteko transferentziak: (Adierazi transferentziak, edo, halakorik ez badago, idatzi hau: «Ez dira nazioarteko transferentziak egingo»).
- Zure datuen gaineko eskubideak hauek dira: sartzea, ezereztea, zuzentzea, aurka egitea, tratamendua mugatzea, transferitzea eta ahaztea. Eskubide horietaz baliatzeko bidali zure eskaera dpd@ehu.eus. helbidera.
- Informazio osagarria eskura dezakezu hemen: http://www.ehu.eus/babestu
- Tratamenduari buruzko informazio osoa hemen: https://www.ehu.eus/es/web/idazkaritza-nagusia/ikerketa-datu-pertsonalen-tratamenduak

Datuen babesari buruzko informazioa horrela aurkezteari ikerketan parte hartuko duten pertsonentzako nahasgarria edo ulertzeko zaila irizten badiozu, haien profilera egokitzen saia zaitezke, baina kontuan hartu oinarrizko informazioan (lehen geruza) ageri diren alderdi guztien berri eman behar duzula.

Sartzeko, Zuzentzeko, Ezerezteko, Aurka Egiteko, Transmititzeko eta Mugatzeko Eskubideei buruzko informazioa (SZEATM)

Eskubideei buruzko informazio honen bidez, datu pertsonalen gaineko *kontrola eta erabakitzeko gaitasuna* bultzatu nahi da. Hori dela eta, ikerketaren arduradun gisa, emaileari informazioa eman behar diozu bere eskubideei, horiek erabiltzeko moduari eta horretarako harremanetan jartzeko moduari buruz:

- **S**artzeko eskubidea edo arduradunari informazioa eskatzeko eskubidea, bere datuak tratatzen ari diren eta, hala bada, zer datu diren jakiteko.
- **Z**uzentzeko eskubidea, edo okerrak edo osatugabeak diren datuak aldatzeko eskatzeko eskubidea.

- **E**zerezteko eskubidea, edo kasu jakin batzuetan datuak ezabatzeko eskatzeko eskubidea; dena dela, lortutako emaitzak ez dira ezereztuko.
- **A**urka egiteko eskubidea, edo zure datu pertsonalen tratamenduaren aurka egiteko eskubidea, zure egoera partikularrari lotutako arrazoiak direla eta.
- **T**ransmititzeko eskubidea, edo datuak erabilera arrunteko eta irakurketa mekanikoko formatu egituratu batean emateko eskatzeko eta beste arduradun bati transmititzeko eskubidea.
- Tratamendua **M**ugatzeko eskubidea, edo datuen tratamendua baldintza jakin batzuetan mugatzeko eskatzeko eskubidea.

NORBERAREN DATU PERTSONALEN GAINEAN ERABAKITZEKO ETA KONTROLATZEKO AHALMENA SUSTATZEA
SZEATM ESKUBIDEAK

SARTZEKO ESKUBIDEA: datuak tratatzen ari ote diren eta zer datu ari diren tratatzen jakiteko.

ZUZENTZEKO ESKUBIDEA: okerrak diren edo osatu gabe dauden datuak aldatzeko.

EZEREZTEKO ESKUBIDEA: suposamendu jakin batzuetan datuak ezabatzeko. Ez dira ezereztuko dagoeneko lortu diren emaitzak.

AURKA EGITEKO ESKUBIDEA: bere egoera partikularrari lotutako arrazoiak direla eta, bere datuak ez tratatuak ez izateko.

TRANSFERITZEKO ESKUBIDEA: datuak erabilera orokorreko eta irakurketa mekanikoko formatu egituratu batean jasotzeko eta beste arduradun bati emateko eskubidea.

TRATAMENDUA MUGATZEKO ESKUBIDEA: bere datuen tratamendua baldintza jakin batzuen arabera mugatzeko.

Ikerketaren arduradun gisa, erakundeak eta INak emaileari informazioa eman behar diote eskubide horiei, horiek erabiltzeko moduari eta horretarako harremanetan jartzeko moduari buruz.

Gordetzeko epeari buruzko informazioa

Aln gordetzeko epeari buruzko informazioa ematean, balizko emaileari adierazi behar diozu gordetzeko gutxieneko epea bost urtekoa dela, datuekin egindako ikerketaren auditoriari eta egiaztapenari begira. Adieraziko diozu, halaber, ikerketarako jasotako datuak gorde ditzakezula horiek ezerezteko eskaera egiten ez duen bitartean eta datu horiek eskuratu zireneko helburuari erantzuten dioten bitartean, eta ezin dizula eskatu ezerezteko eskaera jaso arte bere datuekin lortu diren emaitzak ezerezteko.

Azkenik, gogora ezazu, neurri tekniko egokiak aplikatuz gero —adibidez, anonimizazioa—, datuak denbora gehiagoz gorde ditzakezula.

DATUAK GORDETZEKO EPEA

- Gutxienez *BOST URTE*, ikerketaren auditoria eta egiaztapena egiteko.
- Denbora gehiagoz gorde daitezke ikerketan eskuratu ziren xede berdinerako, non eta ez dagoen ezerezteko eskaerarik.
- Ezin da eskatu eskubide hori erabili aurretik lortutako emaitzak ezerezteko.
- Neurri tekniko egokiak izanez gero (anonimizazioa), denbora gehiagoz gorde daitezke.

Datuen balizko lagapen bati buruzko informazioa

Emailearen datuak hirugarren bati emateko, komunikatzeko eta harekin partekatzeko, emaileak berak lagatzeko aukera horren berri eduki beharko du, hark erabakiko baitu uzten duen ala ez.

Errazena da AI dokumentuaren datuen babesari buruzko atalean, *lagapen eskaera* sartzea, eta hor bertan tarte espezifiko bat uztea *haren adostasuna jasotzeko*. Ez baduzu egin behar, adieraz iezaiozu ez dela *lagapenik* egingo kasu bakar batean ere. Nazioarteko lagapentzat ulertuko da datuak utzi behar direnean Europar Batasuneko lurraldetik

kanpo, edo, Europako Batzordearen arabera, babes maila egokia bermatzen ez duten herrialdeetan.

* Zurekin kontratu bat sinatuta duen *tratamendu eragile* bati (ikus 1. puntua) datuak komunikatzea ez da kontsideratzen datuen lagapentzat, eragile horrek datuak zure jarraibideen arabera bakarrik tratatuko baititu.

Datuen ondorengo tratamenduak edo erabilera gehigarriak

Zera gerta daiteke, emaileak informazioa jaso eta onartu ondoren, ikerketa berri bat planteatzea aurrekoarekin bateragarria den datuen tratamendu berri batekin. Kasu horretan, informazioa posta korreoz, bide elektronikoz edo beste bitarteko batzuen bidez helaraziko diozu, eta aldez aurretik *Ikerketaren Etika Batzordearen* aldeko txostena eduki beharko duzu.

4. Eskatu adostasun esplizitua

> «Interesdunaren borondate-adierazpen aske, zalantzarik gabe, zehatz eta arrazoitua, deklarazio edo egintza positibo argi batez egina, interesduna ukitzen duten datu pertsonalen tratamendua onartzeko dena.» (DBEO, 4.11 artikulua)

Espainiako araudi berrian bereziki babesten diren *osasun datuen* tratamenduei buruzko xedapen espezifiko bat dago (17 XG), eta adierazten du datu horiekin lan egiteko beharrezkoa dela interesdunaren adostasuna eskuratzea, non eta zure ikertaldetik teknikoki eta funtzionalki bereizita dagoen norbaitek seudonimizatzen ez dituen. Hau da, arautzen duenez, ez da nahikoa bermea seudonimizazioa zuk edo zure ikertaldeko kide batek egitea, emailearen adostasunik ez dagoenean.

Osasun ikerketen arloko datu bereziei lotutako eskakizunak eska daitezke ere beste ikerketa arlo batzuetan, datu bereziak diren neurrian (biologia, biomedikuntza, gizarte zientziak, lege zientziak eta portaeraren zientziak). Araudi berria funtsean ez da aldatu, baina zorrotzagoa da berariazko adostasunarekin; izan ere, lehen adostasun tazitua onartzen zen, nahiz eta, egiatan, merkataritza transakzioei egiten zien erreferentzia.

Laburbilduta, legedi berriak adostasunaren beharra indartzen du arau orokor gisa; alabaina, osasun arloko ikerketaren kasuan, ikerketarekin zerikusirik ez duten pertsonek seudonimizatutako datuak erabiltzea ahalbidetzen du. Edonola ere, alderdi hori lagungarria izango zaizu zure ikastegiko DBOren eta IEBren arteko bereizketa zuhurtziaz egiteko.

Adostasunaren ezaugarriak

Datu pertsonalak ematen dituen pertsonaren adostasuna adierazpen libre bat da, non emaileak onartzen baitu bere informazioa eta datuak tratatzea helburu zehatz baterako, lehendik jakinarazi zaizkion baldintza jakin batzuetan.

ESPLIZITUA

ASKEA

INFORMATUA

ARGIA

ESPEZIFIKOA

EGIAZTAGARRIA

BEREIZGARRIA

AGERIKOA

EZEZTAGARRIA

Gaur egun badira oraindik praktika batzuk *adostasun tazitua* izenekoan kokatzen direnak, baina jakin behar duzu dagoeneko ez direla onartzen. Hala, isiltasunak, ez-egiteak edo lehendik aukeratutako laukitxoak ez dute balio dagoeneko adostasuna eskuratzeko modu gisa edo datuak emateko ustezko onarpen gisa. Ongi egintzat hartzen da bakarrik baldintza hauek ematean:

- *Esplizitua:* subjektu emaileak berariazko adostaun adierazpen bat igortzen du (baieztapen ekintza argi bat); adibidez, dokumentu bat sinatzea edo «onartu» ekintza sakatzea ingurune elektroniko batean.
- *Librea:* Askatasunez ematen da, ezin da baldintzatu, esate baterako, lan akademikoaren jaitsiera batera, ondasun material baten lorpenera, edo beste edozein baldintzatara. Adostasuna libreki

eman den ebaluatzean, kontuan hartu behar duzu beti erabaki hori mugatu dezaketen baldintzak ematen ote diren.

- *Informatua:* adostasun benetan informatua izan dadin, balizko emaileak jakin eta ulertu behar du zer esaten ari den, eta horretarako modu ulergarrian adierazi behar diozu, 3. kapituluan azaltzen den moduan.
- *Argia:* adostasuna emateari buruzko informazioak oso argia izan du, eta ez da nahastu behar ikerketari buruzko beste baldintza batzuekin, laginak emateko beste eskaera batzuekin, inkestekin, etab. (Ikus 3. Kapitulua, «nola informatu»)
- *Espezifikoa:* helburu bakoitzerako adostasuna bilatu behar duzu, eta ongi azaldu behar duzu ez duzula erabiliko beste helburu batzuetarako.
- *Egiaztagarria:* tratamenduaren arduraduna zaren neurrian, emaileak bere datu pertsonalak ikerketaren helburuetarako tratatzea onartu zuela probatzeko gai izan behar duzu edozein agintari, pertsona edo batzorde eskudunen aurrean.
- *Bereizgarria eta agerikoa:* Emaileak bere datuak jasotzeko, erabiltzeko eta gordetzeko adostasuna ematen badizu zure ikerketa proiektuan parte hartzeko adostasunaren testuan eta testuinguruan, informazioa beste gaietatik modu argian bereizita aurkeztu behar diozu, modu ulergarrian eta eskuragarrian, eta hizkuntza argia eta soila erabilita.
- *Ezeztagarria:* adostasuna kentzeko aukera eduki behar du une oro, eta adierazi behar diozu hori eskatzea erraza dela eta ondoriorik ez duela; era berean, nola egin behar duen azaldu behar diozu.

DBEO indarrean sartu aurretik eskatutako adostasunaren balioa

Adostasuna 2018ko maiatzaren aurretik lortu bazenuen, ez duzu zertan berriro eskatu adostasuna DBEOren baldintzetan, eman zizutenean arau hori ez zelako aplikagarria. Diligentziaz eta zintzotasunez, ordea, informazio berria ematea gomendatzen dugu, ahal den neurrian.

Euskarri elektronikoan eskuratutako adostasuna

Horrela eskuratutako adostasun informatua paperean lortutakoa bezain baliotsua da, eta dokumentazioa paperean eduki nahi ez baduzu eta nahiago baduzu dena formatu elektronikoan eduki, sinadura digitalaren bidez edo ziurtagiri elektronikoz jaso dezakezu. Gogoratu kasu guztietan emaileak baieztatze ekintza argi bat egin behar duela haren adostasuna baliozkotzat har dadin, eta adostasun horiek, emaileen datuekin batera, babestuta eduki behar dituzula.

Lauki batean klikatuz eskuratutako onarpena —datuen tratamendua onartzen duen ala ez erabakitzeko aukera utzita— adostasun balioduntzat hartzen da, aurrez markatutako laukitxoen bidez egiten EZ baduzu betiere.

Adingabeek emandako adostasuna

Adingabearen adostasuna beharrezkoa da, haren datu pertsonalak biltzeko, erabiltzeko eta gordetzeko; alegia, haren datuak tratatzeko. 14 urtetik gorakoek emandako adostasuna balioduna dela aurresuposatzen da, eta 14 uretik beherakoentzat beharrezkoa da ere gurasoen edo tutoreen baimena. Adingabeen datuak online eskuratu behar badituzu, gogoratu BDOri kontsultatu behar diozula, prozedurak ezarri behar dituzulako gurasoen adostasuna egiaztatu ahal izateko.

5. Aztertu datu pertsonalen tratamenduaren arriskuak eta, hala behar bada, eragin ebaluazio baten beharra

Ikertzaile gisa zure erantzukizuna hartu behar duzu zure gain, eta *segurtasun maila egoki bat* aplikatu beharko duzu, baimenik ez duten pertsonek datuak eskuratzeko, datuak aldatzeko edo suntsitzeko, edo datuak ez eskuratzeko arriskuen arabera.

Horretarako bi tresna dituzu: arriskuaren analisia eta eragin ebaluazioa. Zereginak egiteko UPV/EHUko DBOren aholkularitza jasotzeko aukera izango duzu.

DATUEKIN IZANDAKO GORABEHERAK	BALIOEI EGINIKO KALTEAK
Baimendu gabeko pertsonei ematea…	konfidentzialtasunari
Aldatzea, okerra izatea, manipulatzea…	osotasunari
Galtzea, ezin eskuratzea…	eskuragarritasunari

Arriskuen Analisia (AA)

> DBEOk adierazten du hura betetzen dela bermatzeko neurriek kontuan hartu behar dutela tratamenduaren izaera, arloa, testuingurua eta helburuak, baita pertsonen eskubide eta askatasunerako arriskua ere. Ikuspegi horren arabera, DBEOk ezarritako **neurrietako** batzuk soilik **aplikatuko dira eskubide eta askatasunetarako arrisku handia dagoenean**; beste batzuk, ordea, tratamenduen arrisku maila eta motaren arabera modulatu beharko dira. (AEPD)

Datuen Babeserako Espainiako Agentziak (AEPD) adierazten duen moduan, zure DBOren laguntzaz zure ikerketa nolakoa den, zer testuingurutan egiten den eta zer helburu dituen aztertu behar duzu, tratatuko dituzun datu pertsonalen gaineko eragin negatibo batek horiek ematen dituzten pertsonen eskubideetan eta askatasunetan izan ditzakeen arriskuak ezagutzeko. Gorabehera batek kaltetu ditzakeen informazioaren hiru propietateak honako hauek dira:

1. **Konfidentzialtasuna:** baimenik gabeko pertsonei eman behar ez zaien informazioaren propietatea. Gorabehera posibleak: *ematea, lapurtzea…*
2. **Osotasuna:** aldatua ez izateko eta zehaztasunez gordetzeko informazioaren propietatea. Gorabehera posibleak: *aldatzea, manipulatzea…*
3. **Eskuragarritasuna:** baimendutako pertsonen esku egoteko informazioaren propietatea. Gorabehera posibleak: *eskuratzeko ezintasuna, galera…*

Arriskuen analisia hiru propietate horietako bati uneren batean zerbait gertatzeko probabilitateak aztertzean datza. Hipotesi hauek planteatu behar dituzu: baimendu gabeko pertsonek zure ikerketaren datuak eskuratzea; datuak gaizki manipulatzea, nahigabe edo nahita; eta gorabehera baten eraginez datuak eskuratzeko aukera ez izatea.

Aukera erreal horiek aztertu ondoren (arrisku txikia/arrisku handia), horiek geratuz gero emaileen eskubideetan eman daitekeen kaltea baloratu (arina/larria) behar duzu, eta segurtasun neurri batzuk ezarri (sinpleak/konplexuak), arrisku mota eta mailaren arabera.

UPV/EHUn, Arriskuen Analisia DBOrekin batera egingo duzu, tratamendua erakundearen TJEn erregistratu aurretik, eta kontuan hartuko dira zuk emandako erantzunak, tratamenduan erabilitako bitartekoen eta aplikatutako segurtasun neurrien aurrean. Garrantzitsua da ikertaldeek honako alderdi hauek argi edukitzea:

1. Zuen ikerketan erabilitako datu pertsonalen segurtasunerako izan daitezkeen mehatxuen eszenarioak aztertzea. Esate baterako, adostasun informatu bat paperean parte hartzaileen sinadura daramana beti, eta hura galtzeak edo legez kanpo erabiltzeak identitatea ordezkatzea ekar dezake era guztietako lege dokumentuetan. Gorabeheren beste iturri bat izan daiteke zifratu gabeko datu pertsonalak dituen informazioa bidaltzea ikertaldeko beste ikertzaile batzuei.
2. UPV/EHUren ekipamendu informatiko korporatiboa erabiltzea, segurtasun neurriak ezarrita baititu lehentasun modura. Hori ezinezkoa bada, erabilitako ekipamenduaren segurtasun neurriek erakundeak emandako ekipoak dituenekiko baliokideak izan behar dute.

Eraginaren Ebaluazio bat egitea (DBEE)*

BBOrekin batera Arriskuen Analisia (AA) egin ondoren, ikerketarako behar dituzun datuen tratamenduak pertsonen eskubideentzat *arrisku esanguratsua edo handia* dakarrela ondorioztatuz gero, Eragin Ebaluazio bat egin beharko duzue. Hau da, metodologia jakin baten araberako prozesu sistematiko bat, zure ikerketak datuen babeserako eta horiek eman dituzten pertsonen eskubide eta askatasunerako izan ditzakeen arrisku esanguratsuak aztertzeko. DBOk eskuarki eredu edo programa bat izaten du, prozesu sistematiko hori egitea ahalbidetzen dizuna.

DBEE tresna bat da, arrisku handiko egoeretarako edo bereziki babestutako datu kantitate handiak erabiltzen dituzunerako (DBEOren 35. art.).

DBEEren helburua honako hauek zehaztea da: a) egoera desegokiak gertatzeko *probabilitateak*, b) haien ondorioen *larritasuna* eta c) haien ondorioak saihesteko edo arintzeko hartu beharreko *euspen neurriak*.

Horrela, zure ikerketa proiekturako datuak biltzeko eta erabiltzeko diseinatu dituzun eragiketen *Hasierako Arrisku Maila* ezar dezakezu, eta *Hondar Arrisku Maila Onargarria*, euspen edo segurtasun neurriak bete ondoren.

DBEE horri esker, zehaztu eta deskriba dezakezu hasiera batean zer *segurtasun edo euspen neurri* eta zer *protokolo egoki* aurreikusi dituzun zure ikerketarako beharrezkoak diren datuak jaso, erabili eta gordetzeko une gako bakoitzean izan daitezkeen arriskuak murrizteko, prebenitzeko eta zuzentzeko (probabilitatea eta larritasuna).

DBEE gomendatzea edo nahitaezkoa izatea: DBEEa ez da beti beharrezkoa; alabaina, gomendagarria da, datuak bildu eta erabili behar dituzun aldiro, arriskuen analisi (AA) bat egitea DBOrekin batera, DBEE bat egitearen egokitasuna zehazteko.

DBEEa NAHITAEZKOA da ikerketa mota hauetan:

1. *Arrisku handia:* jasotzea, erabiltzea eta gordetzea oso arriskutsua izan daitezke pertsona fisikoen eskubide eta askatasunetarako. Adibidez, ideologiari edo sexu identitateari lotutako arrazoiengatik emigratu duten pertsonak.
2. *Ebaluazio sistematikoa:* pertsona fisikoen alderdi pertsonalak jasotzen eta ebaluatzen direnean tratamendu automatizatu batean oinarrituta. Adibidez: profilak egitea.
3. *Pribatutasuna inbaditzen duten teknologiak erabiltzea:* ikerketa proiektuan honako hauek erabiliko dira:
    a) Tripulaziorik gabeko aireontziak (dronak).
    b) Datu meatzaritza.
    c) Biometria.
    d) Teknika genetikoak.
    e) Geolokalizazioa.
    f) Bideozaintza eskala handian.
    g) Zaintza elektronikoa.

NAHITAEZKO ERAGIN EBALUAZIOA

Pertsonen eskubide eta askatasunerako arrisku handia duten ikerketak, haien datuak jaso, erabili eta gordetzeagatik. Adibidez, ideologiari edo sexu identitateari lotutako arrazoiengatik emigratu duten pertsonak.

Alderdi pertsonalak tratamendu automatizatu baten bidez sistematikoki ebaluatzen dituzten ikerketak. Adb.: profilak egitea.

Pribatutasuna inbaditzen duten teknologiak erabilita egindako ikerketak:

- Tripulaziorik gabeko aireontziak (dronak).
- Datu meatzaritza.
- Biometria.
- Teknika genetikoak.
- Geolokalizazioa.
- Bideozaintza eskala handian.
- Zaintza elektronikoa.

Bereziki babestutako datuen tratamendua eskala handian egiten duten ikerketak.

Adibidez: datu askorekin, pertsona askori, eremu geografiko zabaletan, pribatutasuna inbaditzen duten teknologiekin, adingabeei eta pertsona zaurgarriei.

4. *Bereziki babestutako datuen tratamendua eskala handian*, esate baterako, honelako ikerketetan:
   - Datu kantitate handia eskatzen dutenak (Datuak jaso, erabili eta gortzeko jardueraren tamaina, barietatea eta iraupena edo iraunkortasuna).
   - Eskualde batean edo hortik gorako esparru geografiko batean egindakoak (datuak jaso, erabili eta gortzeko jardueraren hedapen geografikoa).
   - Pertsona askorengan eragina dutenak (bai termino absolutuetan, bai biztanleria jakin bateko proportzio gisa).

- Datu sentikorrei (biometrikoak, osasunekoak, etab.) buruzkoak eta adingabeen datu pertsonalak dituztenak*.
- Teknologia berriak aplikatzen dituztenak (pribatutasunerako arriskuak izan ditzaketenak) eskala handi horretan.
- Interesdunen eskubide eta askatasunetarako oso arriskutsuak direnak.

DBEEren edukiak[4]

DBEEren azken emaitzak eragin ebaluazioaren txosten bat edo dokumentuen multzo bat izan behar du, eta informazio egokia eman, eta ebaluatutako tratamenduaren eta arriskuen kudeaketaren ezaugarriak jasoko ditu; hau da, arriskuak gutxitzeko zer erabaki hartu diren zehaztuko da. Txosten hori, behin eginda, gainerako dokumentazioarekin batera jasoko da zure ikerketa zehatzean datuen babesari buruz sortutako dokumentuen fitxategi batean, zeina zure DBOk emango baitizu.

ERAGINAREN EBALUAZIO TXOSTEN horrek izango ditu:

1. *Proiektuaren analisia:* bertan zehaztuko dira berriro bildu, erabili eta gordeko dituzun datuen kategoriak, horiek eskuratzeko aukera izango duten pertsonak, informazio jarioak, eta erabilitako teknologiak (1. kap.).
2. *Proportzionaltasun irizpena:* bertan zehazten da ea lortu nahi duzun helburua beste bitarteko batzuen bidez lor daitekeen, esate baterako, beste datu batzuk edo datu gutxiago erabiliz, emaileen kolektiboa maila kuantitatiboan edo kualitatiboan murriztuz, teknologia ez hain inbaditzaileak erabiliz, tratamendurako beste prozedura edo bitarteko batzuk erabiliz, etab. Irizpen hori lehen fasean (1. kap.) dagoeneko landutako eta berrikusi beharreko hiru alderdi hauetan oinarritzen da:

[4] **Datuak Babesteko Espainiako Agentziaren gida.** AEPDk Datu Pertsonalen Babesean eragin ebaluazio bat egiteko **gida** bat argitaratu du bere webgunean. Dokumentua laguntza handikoa da DBEEak egiteko.

a) Egokitasuna: jasotako datuek ikerketan proposatutako helburua lortzeko balio dute.

b) Beharra: ez dago hori baino era neurritsuago bat ikerketa eraginkortasun berberaz egiteko.

c) Proportzionaltasuna: haztatua edo orekatua da, interes orokorrerako onura edo abantaila gehiago eratortzen direlako tartean diren ondasun edo balioen gaineko kalteak baino.

3. *Arriskuen ebaluazioa:* atal honetan eraginpeko datuak babesteko egon daitezkeen arriskuak aztertzen dituzu, aurreko puntuetan dagoeneko berretsi duzulako beharko dituzula. Horiek emateko probabilitatea baloratuko duzu, baita, gertatuz gero, eragina ere.

4. *Aurreikusitako neurriak:* Arriskuei aurre egiteko, zure DBOk aholkatuta, ezarri beharreko neurriak jaso behar dituzu.

Ikusten duzun moduan, *DBEE on* bat eta *DBEE txosten* egoki bat egiteko, ezinbestekoa da Datuen Babeserako Ordezkariaren (DBO) lankidetza (dpd@ehu.eus), bai ebaluazioaren diseinuan eta exekuzioan partaidetza aktiboa edukita, bai koordinazio zereginak beteta edo ebaluatzailearekiko solaskide nagusia edo kolaboratzailea izanda.

Kontuan hartu DBEE bat egitea nahitaezkoa dela ikerketaren izaeraren, metodologiaren eta bitartekoen arabera. UPV/EHUn, Datuen Babeserako ordezkariari tratamendua UPV/EHUren TJEn sartzeko eskaera egiteko inprimakiak DBEE bat egitearen beharra ebaluatzen du, zuk bertan emandako informazioaren arabera. Tratamenduaren eragin maila estimatuaren azpian, «TRATAMENDU HONETARAKO ERAGIN EBALUAZIO BAT EGIN BEHAR DA» esaldia agertzen denean nahitaezkoa da inprimaki horren 16. atalari erantzutea, bere horretan DBEE bat baita. Hori guztia baino hobe da, ordea, alderdi etikoak eta metodologikoak berriro planteatzea, ikerketak parte hartzaileen pribatutasunean eta eskubideetan eragin maila txikiagoa izan dezan. Askotan ezin da, eta orduan zintzotasunez birplanteatu behar da ikerketarako pentsatutako metodologiaren pertinentzia, emaileen eskubide eta pribatutasunerako duen arriskuaren aurrean. Erantzuna baiezkoa bada, haren justifikazioa DBEE bera da, eta ahal bezain arrazoitua eta xehea izan behar du.

Online (hodeian) biltzea, erabiltzea eta gordetzea

Ikerketarako datuen tratamendua online egiteko, hala nola *cloud computing* edo konputazioa hodeian, ebaluazio on bat egin behar duzu, eta neurri egokiak hartu behar dituzu:

- Datu horiek *hodeian tratatzeari lotutako arriskuak.*
- *Arriskuak minimizatzeko neurriak hartzea*, hala nola seudonimizazioa edo anonimizazioa, baita makrodatuak edo Big data tratatzen dituztenean ere[5].
- Jasotzea eta ebaluatzea hodeiko zerbitzuaren baldintzak zein diren, eta arau eskakizunak (adb., datuen kokaleku fisikoa: legez «segurua» den espazio batean dauden) eta segurtasun neurriak (adb., informazioaren zifratzea online trantsituan) betetzen diren.
- Kontratu bat sinatzea hodeian zerbitzuak ematen dituenarekin (unibertsitatea ez denean); izan ere, «tratamendu eragiletzat» hartuko da, eta horren barruan, zerbitzuak amaitzean, datuak zerbitzua kontratatu duen ikerketaren arduradunari itzultzeko baldintza sartuko da.

[5] Big Data (Makrodatuak): Hainbat gailuren bidez (mugikorrak, kirolerako eskumuturrak, ordulari adimendunak, ordenagailuak, etab.) gure ohiturei, ordutegiei eta abarrei buruz jasotako datu kantitate andana batek eratzen dute Big Data. Horren bidez, enpresek datu multzoak aztertzen dituzte; hala, datuak moldatu edo probatu daitezke, joerak bilatzen dira, arlo korapilatsuak detektatu daitezke, etab. Eskuarki, Big Datan datu guztiak anonimizatuta egoten dira; beraz, datu horien bidez ezin da pertsona jakin bat identifikatu; halere, anonimazioa itzulgaitza izan dadin aplikatu beharreko segurtasun neurriak ezarri behar dira. **Datu pertsonalen anonimizazioa** eraginpeko pertsonari identifikatzea ahalbidetzen duen informazioa mugatzea eta ezabatzea da. Helburu nagusia da datuak berriro erabiltzean pertsona hori identifikatzeko aukera behin betiko saihestea da.

6. Bermatu segurtasuna

DBEOren 5.1.f artikuluak zehazten du beharrezkoa dela segurtasun neurri egokiak ezartzea, funtsean, honako hauek saihesteko:

- Eskatu dituzun datu pertsonalak baimenik gabe edo legez kanpo erabiltzea
- Datu pertsonal horiek galtzea, suntsitzea edo kaltetzea.
- Datuak eskuratzeko aukerarik ez izatea.

Halakorik ez gertatzeko, neurri teknikoak eta antolakuntzakoak ezarri behar dituzu osotasuna, konfidentzialtasuna eta eskuragarritasuna ziurtatzeko, eta gainera, horiek ikerketa egin bitartean eta ondoren martxan dituzula erakusteko aukera emango dizute (ikuskaritza baten harira eskatzen denean). DBOk horren inguruan aholkatuko dizu.

Antolakuntzako segurtasun neurriak

Zure ikertaldeko pertsona guztiek jakin behar dute, alde batetik, konfidentzialtasun betebehar bat dutela, ikerketa amaitu ondoren ere bere horretan mantenduko dena, eta, bestetik, datuok baimendu gabeko pertsonen esku uztea saihestu behar dutela. Komenigarria da datuak eskuratuko dituzten guztiek konfidentzialtasun dokumentu bat izenpetzea.

Betebehar horiek modu eraginkorrean gauzatzeko, ezarri beharreko proiektua diseinatzean, antolakuntza neurri hauek finkatu behar dituzu:

1. Gomendagarria da datuen tratamendurako segurtasun neurri batzuk hartzea, ikertalde osoak ezagutuko dituena. Gure kasuan, arau horiek bateragarriak izan behar dute UPV/EHUren

Informazioaren Segurtasun Politikarekin (AKORDIOA, 2013ko apirilaren 25ekoa, UPV/EHUren Gobernu Kontseiluarena, Universidad del País Vasco/Euskal Herriko Unibertsitatearen Informazioaren Segurtasun Politika onartzeari buruzkoa).

2. *Rolak eta erantzukizunak,* bereziki nor izango den segurtasunaren arduraduna.
3. Ordenagailuen, softwarearen, biltegiratze gailuen eta sareko baliabideen kudeaketa.
4. *Ohiko segurtasun neurriei buruzko prestakuntza:*
    - Datu pertsonalak ez uztea hirugarrenek eskuratzeko moduan (zaindu gabeko pantaila elektronikoak, datu pertsonalak dituzten paperezko dokumentuak sarbide publikoetan, etab.).
    - Alde egin aurretik, pantaila blokeatzea edo saioa ixtea; paperezko dokumentuak eta euskarri elektronikoak leku seguruetan gordetzea (sarrera mugatuko armairuak edo gelak) egunaren 24 orduan.
    - Datuak edo informazio pertsonala ez komunikatzea hirugarrenei; bereziki, telefono kontsultetan, posta elektronikoetan, etab.
5. Datuak eman dituen pertsonarentzat *erantzun eta sarbide prozedura seguruak* ematea, eskubideak erabili nahi dituenean: bitarteko elektronikoak, IN edo DBOrengana bideratzea, posta helbidea, etab.
6. *Segurtasun urraketa baten aurrean jarduteko protokoloa:* Datu pertsonalak modu desegokian eskuratzen, informazioa aldatzen edo sarrera bat galtzen denean, harremanetan jarri behar duzu berehala zure DBOrekin, gorabehera erregistratzeko eta haren ondorioak ebaluatzeko. Segurtasunean izandako arrakalak pertsona fisikoen eskubide eta askatasunetarako arrisku bat ekar badezake, atzerapenik gabe informatu behar diezu pertsona horiei eta erakundeari (UPV/EHU, gure kasuan) DBOren bidez, eta Datuen Babeserako Espainiako Agentziari ere jakinarazi beharko diozu 72 orduan gehienez ere, gertaerak argitzeko beharrezkoa den informazio guztia emanda haren egoitza elektronikoaren bidez (https://sedeagpd.gob.es)

ANTOLAKUNTZAKO SEGURTASUN NEURRIAK IKERTALDEARENTZAT

- Ezarri taldearentzat segurtasun arau batzuk datuen tratamendurako.
- Banatu rolak: bereziki nor izango den segurtasunaren arduraduna.
- Antolatu ordenagailuen, softwarearen, biltegiratze gailuen eta sareko baliabideen kudeaketa.
- Bete ohiko segurtasun neurriak:

  1. Ez utzi datu pertsonalak hirugarrenek eskuratzeko moduan (zaindu gabeko pantaila elektronikoetan, sarbide publikoko eremuetan utzitako paperezko dokumentuetan, datu pertsonalak dituzten gailuetan, etab.).
  2. Joan aurretik blokeatu pantaila edo saioa itxi.
  3. Gorde beti paperezko dokumentuak eta euskarri elektronikoak oso leku seguruetan.
  4. Ez komunikatu datuak edo informazio pertsonala hirugarrenei, bereziki telefono kontsultetan, posta elektronikoetan, etab.

- Ezarri datuak eman dituen pertsonarentzako erantzun eta sarbide prozedura seguruak, eskubideak erabili nahi dituztenean: bitarteko elektronikoak, IN edo DBOrengana bidaltzea, posta helbidea, etab.
- Datuak modu desegokian eskuratzen, informazioa aldatzen edo sarrera bat galtzen denean, jar zaitezte harremanetan berehala zuen DBOrekin.

Segurtasun neurri teknikoak

Neurri teknikoak arriskuak saihesteko edo minimizatzeko oinarrizko segurtasun neurriak dira, eta maiztasun batez berrikusi behar dira, modu automatikoan (softwarea edo programa informatikoak) edo eskuz:

1. *Sarbide kontrola eta autentifikazioa: profilak eta pasahitzak:*

    a) Eduki hainbat erabiltzaile edo profil desberdin helburu bakoitzerako: ordenagailu edo tresna bera erabiltzen duzuenean ikerketaren datu pertsonalak tratatzeko eta beste helburu pertsonal edo profesionaletarako, erabilera horiek bereizita edukitzea gomendatzen dugu.

    b) Eduki instalazioa administratzeko eta sistema konfiguratzeko eskubideak dituzten profilak eta datu pertsonalak eskuratzeko administrazio pribilegioak edo eskubideak ez dituzten erabiltzaileen profilak: neurri horren bidez, zibersegurtasunaren aurkako eraso batean aurrean, sarbide pribilegioak eskuratzeko edo sistema eragilea aldatzeko aukera saihestuko duzu.

    c) Bermatu sistema elektronikoetan gordetako datu pertsonalak eskuratzeko pasahitzak daudela; gutxienez 8 karakterekoak izango dira, zenbakiak eta letrak nahastuta.

    d) Identifikazio argia: hainbat pertsona datutara sartzen direnean, eman erabiltzaile eta pasahitz espezifiko bat bakoitzari.

    e) Pasahitzak: pasahitzen konfidentzialtasuna bermatu behar duzu, hirugarrenen esku geratzen direla saihestuta. Pasahitzak ezin dira partekatu, inola ere, ezta idatzita utzi ere erabiltzaile ez diren pertsonek sartzeko aukera duten lekuetan.

2. *Sarrerak erregistratzeko artxiboa: jarduera, monitorizazioa eta jarraipena:*

    a) Sarrerak erregistratzeko artxiboen erabilera segurtasun neurri garrantzitsu bat da, eta datu pertsonalekin egindako ekintzen identifikazioa eta jarraipena egitea ahalbidetzen du.

3. *Segurtasuna lanpostuetan, zerbitzarietan eta sareetan:*

    a) Eguneratzea: ahal den neurrian, ordenagailuak eta tresnak eguneratuta daudela ziurtatu behar duzu.

    b) Antibirusa: datu pertsonalen tratamendu automatizatua egiten duzun ordenagailuetan eta gailuetan eduki antibirus sistema bat, eta eguneratu maiztasun batez.

    c) Zifratzea: sarearen segurtasuna garrantzitsua da, bai kanpo konexioetan (esate baterako, Internet), bai unibertsitatearen beste sistema (kanpokoak nahiz barrukoak) batzuekiko konexioetan. Sarrera Internet bidez egiten duzunean, zifratu informazioa protokolo kriptografikoak erabilita (TLS/SSL).

    d) Suebakiak eta sarkinak detektatzea: monitorizatu trafikoaren joan-etorria informazio sisteman, suebakiak eta sarkinak detektatzeko sistemak erabilita.

    e) Segregazioa: datuen sarea beste sareetatik bereizi behar da.

4. *Datuak zifratzea:*

    a) Datu pertsonalak bitarteko fisikoak edo elektronikoak erabilita mugitu behar dituzunean, erabili zifratze metodo fidagarri bat.

5. *Segurtasun kopiak:*

    a) Segurtasun kopia bat egin maiztasun batez beste gailu batean, eguneroko lanerako erabiltzen duzunaz aparte. Gorde kopia leku seguru batean, fitxategi originalak dituen ordenagailua dagoen lekuaz aparte; horrela, informazioa galduz gero, datu pertsonalak berreskuratu ahal izango dituzu.

6. *Gailuak modu egokian suntsitzea eta datuak ezabatzea.*

7. *Instalazioen segurtasun fisikoa.*

Bistan da ikertalde guztiak prestatu eta entrenatu beharko direla horrelako lanetan, beren proiektuak aurrera atera ahal izateko. Garrantzitsua da hori guztia ikerketaren diseinuan bertan planteatzea, denbora, lana, baliabide materialak eta giza baliabideak behar baitira. Zorionez, zure ikastegian DBOren laguntza izango duzu beti, hori baita haren jakintza arloa eta eskumena.

7 SEGURTASUN NEURRI TEKNIKO IKERKETA EGIN BITARTEAN

1. Sarreraren kontrola eta autentifikazioa: profilak eta pasahitzak.
2. Sarrerak erregistratzeko artxiboa: jarduera, monitorizazioa eta jarraipena.
3. Segurtasuna lanpostuetan, zerbitzarietan eta sareetan:
   - Eguneratzea.
   - Antibirusa.
   - Zifratua.
   - Suebakiak eta sarkinak detektatzea.
   - Datuen sarea beste sareetatik bereiztea.
4. Datuak zifratzea.
5. Segurtasun kopiak egitea.
6. Gailuak modu egokian suntsitzea eta datuak ezabatzea.
7. Instalazioen segurtasun fisikoa.

7. Dokumentatu diligentziaz

Zure ikerketaren alderdi jakin honen egiaztatze eta kontrol lana amaitzeko, beharrezkoa da hainbat dokumentu prest eta gordeta edukitzea, hala nola adostasunak sinatuta, interesdunen eskubideen balizko erabilera, gorabeheren kudeaketa, konfidentzialtasun konpromiso sinatua eta, hala behar izanez gero, tratamendu eragileen kontratuak. Dokumentu batzuk tratamendua erregistratzeko prozesuan edo zure DBOrekin egindako kudeaketetan sortzen dira, eta ez da beharrezkoa zuk horiek pertsonalki gordetzea. Hurrengo ataletan dokumentuak aipatzen dira, nork sortzen dituen, nola sortzen diren eta non gorde behar diren adierazita.

Ikerketa proiektuaren arduraduna zaren neurrian, datu pertsonalen babesari lotutako erantzukizunak betetzean diligentziaz jardun duzula erakusteko gai izan behar duzu. Horretarako onena da datu horien inguruan egindako lanak dokumentuetan jasotzea.

1. Tratamendu Jardueren Erregistroa (TJE).
2. Adostasunak gordetzea.
3. Eskubideen erabilera erregistratzea.
4. Arriskuen analisiari buruzko txostena.
5. Eragina ebaluatzeko txostena (DBEE).
6. Gorabeheren kudeaketa erregistratzea.
7. Isilpekotasun konpromisoak.
8. Tratamendu eragileen kontratuak.
9. Ikerketa proiektuaren segurtasun arduradunaren izendapena.

Ikerketa guztietan ez dituzu beharko dokumentu horiek guztiak, baina denak posibleak dira, legediaren arabera.

1. dokumentua. **Tratamendu Jardueren Erregistroa (TJE)**

Tratamendu Jardueren Erregistroa nahitaezko dokumentu bat da, eta bertan, erakundeak egiten dituen datu tratamenduen zerrenda jasotzen da, tartean egonda, besteak beste, ikerketa proiektuei lotutako tratamenduak. Gure kasuan, TJE formatu elektronikoan dago, eta UPV/EHUren webgunean kontsulta daiteke www.ehu.eus/babestu

DBOri zure ikerketari lotutako datuen tratamendua erregistratzeko eskatu ondoren, hura TJEn sartuko da (UPV/EHUrena edo dena delako erakundearena). Ez da beharrezkoa TJEn dituzun tratamenduen zerrenda bat eramatea, baina komeni da.

Bigarren informazio geruzari dagokion tratamenduaren informazioa gordeko da TJEn.

2. dokumentua. **Adostasunak gordetzea**

Ikertzaile nagusi arduraduna zaren neurrian, datuen tratamendurako emaileen adostasun guztiak gorde behar dituzu, formatu elektronikoan edo paperean. Dokumentu horiek tratamendu hori egiteko legitimotasuna erakustea ahalbidetuko dizute, hala behar izanez gero. Hala paperean nola formatu elektronikoan, modu seguruan gorde behar dituzu tratamenduaren adierazpen inprimakian zehaztu beharko duzun leku batean. Zure DBOk hori egiteko moduaz aholkatuko dizu.

3. dokumentua. **Eskubideen erabilera erregistratzea**

Zure ikerketan parte hartzen duten pertsonek beren SZAETM eskubideak erabil ditzakete DBOren bidez (UPV/EHUkoa, gure kasuan). Pertsona horiek INrengana edo ikertaldeko beste kide batengana jotzen dutenean, berehala jakinarazi beharko diozu DBOri, zeinak eskubideak erabiltzeko jasotako eskaera guztiak eta horiei emandako erantzunak erregistratuko baititu. Erregistro hori DBOk tratamendua erregistratzeko unean emandako helbide elektroniko berean kokatuko da.

4. dokumentua. **Arriskuen analisiari buruzko txostena**

Arriskuen analisiari buruzko txostena eguneratuta eduki behar da, eta arriskuen analisia, haren ondorioak eta hartutako segurtasun neurriak dokumentatu behar ditu. Dokumentu hori ere TJEn sartzen da tratamenduaren erregistroa baino lehen, eta DBOk esleitu dizun plataforman edo artxiboan jarri behar duzu.

5. dokumentua. **Eragina Ebaluatzeko Txostena (DBEE)**

Dakizun moduan, arrisku handia duten edo bereziki babestutako datuen tratamendu masiboa eskatzen duten ikerketa proiektuetan nahitaezkoa da txosten hori edo horiek egitea (gerta baitaiteke bat baino gehiago egin behar izatea ikerketa proiektuan izandako aldaketengatik).

Dokumentu hori tratamenduaren adierazpen inprimakian sartuta dago, eta DBOk esleitutako TJEn sartu behar duzu, tratamendua erregistratu aurretik.

6. dokumentua. **Gorabeherak kudeatzeko erregistroa**

Dagoeneko aipatu dugunez, datu pertsonalei eragiten dien egoeraren bat ematen denean harremanetan jarri behar duzu zure DBOrekin, eta horrek segurtasuneko gorabehera erregistratu behar du, eta, hala behar bada, Datuen Babeserako Espainiako Agentziari jakinarazi behar dio.

Komenigarria da gorabehera horien erregistroa egitea, bertan jasotzeko gorabeheraren deskribapena, datuak, kaltetutako pertsonak, ondorioak, eta hartutako neurriak. Erregistro hori zure ikerketa diseinatzean datuen tratamendua erregistratu zenuenean DBOk esleitutako helbide elektroniko edo plataforma berean kokatuko da.

7. dokumentua. **Konfidentzialtasun konpromisoa**

Zure ikerketaren datu pertsonalak eskuratzen dituzten pertsonek sinatutako konfidentzialtasun konpromiso guztiak gordeta eduki beharko dituzu, formatu elektronikoan (sinadura elektronikoa behar da) edo paperean. Dokumentu horiek ere tratamendua erregistratu zenuenenean Datuen Babeserako Ordezkariak (DBO) emandako helbide elektroniko edo plataforma berean kokatuko dira.

8. dokumentua. **Tratamendu eragileen kontratuak**

Tratamendu eragileen kontratuak, halakorik balego, sinatuta jaso eta gorde behar dituzu, formatu elektronikoan (sinadura elektronikoa behar da) edo paperean. Gure erakundean, esate baterako, kontratu eredu ofizial bat dugu www.ehu.eus/babestu helbidean («*UPV/EHUren aginduz datuak tratatzen dituzten kanpoko enpresek hartu beharreko konpromisoak», Gobernu Kontseiluak 2008ko apirilaren 10eko bileran onartutakoa)*. Gainerako dokumentuak bezala, hauek ere DBOk emandako plataforman edo helbide elektronikoan jaso behar dira.

9. dokumentua. **Ikerketa proiektuaren segurtasun arduradunaren izendapena**

Azaldu dugun moduan, gomendagarria da ikertaldeko kide bat segurtasun arduradun izendatzea, eta hori dokumentu batean jasota geratzea, non adieraziko baita nor den, eta nola onartu eta bereganatu dituen bere erantzukizunak). Gainerako dokumentuak bezala, izendapen horrek ere jasota geratu behar du zure DBOk emandako plataforman edo helbide elektronikoan.

8. Eranskina

Adostasun informatua, ikerketan parte hartzeko eta laginak edo datuak erabiltzen uzteko eskatzeko

Gizakiekin edo haien lagin edo datuekin ikerketa bat abiarazteko, nahitaezkoa da parte hartzeko borondate libre eta kontzientearen adierazpen bat edukitzea, ahalmena duten pertsonek edo baimendutako ordezkariek modu baliodunean emango dutena, informazio egokia jaso ondoren (LIB art. 3f).

Adierazpen hori emateko, parte hartzaile bakoitzari ikerketari buruzko informazio egokia emango zaio, eta soilik horrela erabakiko du. Datuak eskatzen bazaizkio, horri buruzko informazio espezifikoa sartu beharko da, eta, ikerketa batean parte hartzeko haren adostasuna jasotzeaz gainera, atal espezifiko batean bere datuak erabiltzeko adostasuna jasoko da, indarrean dagoen legediak eskatzen duen moduan.

ADOSTASUN INFORMATUKO DOKUMENTU BATEN OINARRIZKO EGITURA

ERAKUNDEAREN LOGOA (gure kasuan UPV/EHU)

IKERTZAILE ARDURADUNA IDENTIFIKATZEA

- Izen-deiturak.
- Saila eta ikastegia.
- Harremanetarako datuak: helbide elektroniko eta telefono zenbaki instituzionalak.

IKERKETAREN DESKRIBAPENA (Nahitaezko gutxieneko informazioa)

- Proiektuaren identifikazioa: Izena eta finantzaketa.
- Proiektuaren laburpena:
  - — Helburuak eta espero diren onurak.
  - — Iraupena.
  - — Egingo den lekua.

Errekrutatutako subjektuarekin egin beharreko **ESKU HARTZEEN DESKRIBAPENA:**

- Proba edo esku hartze mota eta deskribapena (inkesta, lagina hartzea, audioa grabatzea, bideoa…) eta haren helburua.
- Zenbat aldiz egingo den; datak eta epeak.
- Gero parte hartzailearekin harremanik egongo ote den.
- Arriskuen eta/edo eragozpenen deskribapena eta horiek gutxitzeko neurriak (asegurua barne, hala badagokio).
- Zalantzak argitzeko eta informazio gehiago emateko eskaintza, eta horretarako harremanetan jartzeko modua zehaztea.

BOLUNTARIOTASUNA

Parte hartu nahi duen ala ez erabakitzen du. Jakinarazten zaio parte hartzea borondatezkoa dela eta ezetz esateak ez dakarkiola inolako kalterik edo kontrako neurririk.

BALIOGABETZEA

Jakinarazten zaio ikerketatik atera daitekeela nahi duenean, inolako ondorio pertsonalik izan gabe eta azalpenak emateko beharra izan gabe. Jakinarazten zaio, halaber, norekin (IN) kontaktatu behar duen eta zein den erakundearen harremanetarako helbidea, baliogabetzea aurrera eramateko.

ZER EGIN LAGINEKIN

Ikerketa amaitzean bere laginekin zer egin daitekeen adieraziko zaio, erabaki dezan:

- Suntsitzea.
- Anonimizatzea.
- Doan ematea Biobanku bati, hura identifikatuz.
- Laginen bilduman kontserbatzea, hasieran proposatutakoarekin lotura duten ikerketetarako.
- Bestelakorik.

HAREN DATUAK BABESTEA

Datu pertsonalak ematen dituenean, Datuen Babeserako Europako Erregelamenduaren (EU2016/679) arabera, informazio hau emango zaio:

Datu pertsonal hauek eskatzen dira: . . . . . .
Datuen tratamenduaren kodea hau da: . . . . . .
Datuen tratamenduaren izena hau da: . . . . . .
Tratamenduaren helburua da: . . . . . .

Datuen tratamenduaren arduraduna da:

Gure kasuan, UPV/EHU agertuko da: Universidad del País Vasco/ Euskal Herriko Unibertsitatea. IFK: Q4818001B. Posta helbidea: Sarriena auzoa z/g, 48940-Leioa (Bizkaia). Webgunea: www.ehu.eus. Datuen Babeserako ordezkariarekin harremanetan jartzeko datuak: dpd@ehu.eus.

Datuak gordetzeko epea izango da: . . . . . .

Tratamenduaren legitimazioa haren adostasun informatua da.

Datuak nazioartean uzteko eta transferitzeko aukerak, utziko diren ala ez eta, hala bada, nori utziko zaizkion adierazita.

Lagapenak

EZ: «Informazio hau ez du eskuratutako proiektutik kanpo dagoen inork, legezko betebehar bat betetzeko ez bada.»

BAI: «Zuk emandako informazioa beste ikertzaile eta unibertsitate batzuek eskuratu ahal izango dute (nork eta zergatik adierazita)»

Nazioarteko transferentziak

EZ: «Datuak ez dira transferituko Europar Batasunetik kanpoko herrialdeetara».

Bai: «Datuak Europar Batasunetik kanpoko herrialdeetara transferituko dira».

Datuen gaineko eskubideak hauek dira: sartzea, ezereztea, zuzentzea, aurka egitea, tratamendua mugatzea, transferitzea eta ahaztea.

Gure kasuan, eskubide horietaz baliatzeko bidali zure eskaera dpd@ehu.eus. helbidera. Informazio osagarria duzu hemen:http://www.ehu.eus/babestu. Tratamendu honi buruzko informazio osoa, berriz, hemen: https://www.ehu.eus/es/web/idazkaritza-nagusia/ikerketa-datu-pertsonalen-tratamenduak

Zer egin datuekin: Behin ikerketa amaituta, horretarako utzitako datuekin zer egingo den adieraziko da:

- Suntsitzea.
- Anonimizatzea.
- Lagatzea, nori identifikatuta.
- Gordetzea, hasieran proposatutakoarekin lotura duten ikerketetarako.
- Bestelakorik.

DOAKOTASUNA

Jakinarazten zaio parte hartzea (datuak eta laginak emanez, inkestei erantzunez, etab.) altruista dela eta, beraz, ez zaiola ordainsaririk emango. Konpentsazioren bat izanez gero, deskribatu egingo da.

IKERKETAREN EMAITZAK ESKURATZEA

Jakinaraziko zaio ikerketaren emaitzak ezagut ditzakeela eta horretarako harremanetan jarri beharko dela ikerketaren arduradunarekin.

Datu genetikoen kasuan, aukera hauek jakinaraziko zaizkio:

- Ezustean eman daitezkeen aurkikuntzak.
- Ez jakiteko eskubidea.
- Familientzako informazioa.
- Kontseilu genetikoa.

IKERKETAN PARTE HARTZEKO ADOSTASUN SINADURAK

- Adostasun dokumentuaz informatzeko eta hura biltzeko ardura duen pertsonaren identifikazioa, data eta sinadura.
- Ikerketan parte hartzeko adostasuna ematen duen pertsonaren identifikazioa, data eta sinadura.
  - — 12 urtetik beherakoa: lege ordezkariaren identifikazioa eta sinadura.
  - — 12-18 urte bitartekoa: Lege ordezkariaren identifikazioa eta sinadura eta adingabearen identifikazioa eta baieztapena.

DATUEN TRATAMENDURAKO ADOSTASUN SINADURAK

- Bere datu pertsonalak dokumentu honen ZURE DATUEN BABESA puntuan deskribatutako baldintzetan erabiltzea baimentzen duen pertsonaren identifikazioa eta sinadura.
  - — 12 urtetik beherako adingabeak: lege ordezkariaren sinadura.
  - — 12-14 urte arteko adigabeen datuak: lege ordezkariaren sinadura, eta adingabearen adostasuna.
  - — 14 urtetik gorako adingabeak: adingabearen sinadura.
  - — 18 urtetik beherako adingabearen datuetarako ikerketa inbaditzaile batean (arrisku psikikoa horiek lortzean): lege ordezkariaren sinadura, eta adingabearen adostasuna.

Guía de protección de datos en investigación con seres humanos

Basada en el nuevo Reglamento Europeo de Protección de Datos (RGPD) y Ley Orgánica 3/2018 de Protección de datos personales y garantía de los derechos digitales (LOPD-GDD)

Índice

Presentación

La protección de datos personales obedece a la voluntad de proteger la libertad y la vida privada de las personas. Es una tarea éticamente valiosa que se ha plasmado en leyes concretas y esto es preciso tenerlo siempre presente, para actuar con responsabilidad y no solo por cumplimiento de la legalidad. Cuando se interioriza esta convicción es más sencillo resolver las dudas y situaciones concretas en torno a la protección de datos y en consecuencia, cuidar adecuadamente la privacidad y la autonomía de las personas.

USO DE DATOS PERSONALES EN INVESTIGACIÓN: es responsabilidad de quienes investigáis, proteger a quienes han accedido a ser sujetos de investigación; tanto en la investigación que requiere el uso de datos personales, como en la que se necesitan muestras biológicas humanas o de la participación directa de personas voluntarias.

Este breve manual pretende facilitaros el cuidado que debemos a los sujetos fuente o donantes de datos que vamos a utilizar en nuestras actividades de investigación, bien sea investigación básica, aplicada o tutelada como tesis doctoral, trabajos fin de máster o trabajos fin de grado. Este cuidado que debemos a los sujetos participantes o donantes se concreta en la protección de su intimidad, privacidad y libertad, promoviendo la confidencialidad y el cumplimiento de la legalidad vigente.

Estas son las cuestiones a las que tenéis que responder al diseñar un proyecto, antes de poner en marcha vuestra actividad de investigación, si vais a necesitar datos de personas.

20 preguntas básicas para organizar tu proyecto de investigación

1. ¿Cómo se llama tu actividad de investigación?
2. ¿Necesitas que algunas personas te proporcionen información suya para llevarlo a cabo?
3. ¿Qué tipo de datos concretos necesitas?
4. ¿Con qué fin, desde el punto de vista metodológico, necesitas esos datos?
5. ¿Obtendrás esos datos directamente de las personas?
6. ¿A través de qué mecanismos (encuesta, entrevista, historia clínica) vas a extraer y recoger los datos?
7. ¿Has elaborado un documento con información concreta, suficiente y veraz para explicarles lo que vas a pedirles a las personas donantes y para qué vas a utilizar esa información?
8. ¿Has incluido en el documento la información sobre cuáles son sus derechos y la posibilidad de que los ejerzan?
9. Si te proporcionan los datos otras fuentes que no son las personas donantes ¿cómo lo harán?
10. ¿Cuándo tengas los datos, los *seudonimizarás* haciendo una separación de los datos y las identidades con códigos, para evitar la identificación personal?
11. ¿Dónde vas a guardar los datos y a trabajar con ellos, mientras dure tu investigación?
12. ¿Quiénes vais a poder acceder y usar los datos para llevar a cabo el trabajo de investigación?
13. ¿Cuánto tiempo vas a necesitar trabajar con esos datos y conservarlos después?
14. ¿Tienes previsto ceder los datos a personas ajenas a tu equipo de investigación?
15. ¿Qué perjuicios podría suponer para las personas que te han donado sus datos que se te perdieran o que alguien los usara ilícitamente?
16. ¿Qué perjuicios supondría para la investigación que no pudieras acceder a los datos recogidos?
17. ¿Qué mecanismos has previsto para que no los usen ilícitamente?, ¿y para que no se te extravíen? ¿y para que no se te bloquee el acceso?
18. ¿Has establecido algún protocolo, documento o tutorial para trasmitir a todo tu equipo las necesidades y obligaciones de protección que genera el utilizar esos datos de personas?
19. ¿Tienes preparado algún documento para registrar todo lo que estás haciendo en relación con la protección de la información recogida para tu investigación?
20. ¿Te has puesto en contacto con la persona delegada de protección de datos (DPD) de tu institución para que te ayude a pensar y a hacer bien todo lo relacionado con la protección de datos?

Las respuestas a estas preguntas, desde las exigencias de la normativa, se pueden resumir en siete pasos:

1. **Identifica diez aspectos básicos:** (1) Si son datos personales, (2) la finalidad que quieres darles, (3) su procedencia, (4) las personas interesadas (reclutadas/donantes), (5) si son datos especiales, (6) los tratamientos que vas a realizarles (7) las personas responsables de ello (8) las posibles cesiones a terceros y (9) las posibles transferencias internacionales. (10) Ponte en contacto con el DPD.
2. **Actúa con licitud** cumpliendo con las condiciones para un *tratamiento legítimo*[1] de los datos personales en investigación, particularmente si son datos especiales. En actividades de investigación, normalmente la legitimación del tratamiento es el Consentimiento Informado de los donantes de los datos, aunque excepcionalmente pueden existir otras fuentes de legitimación.
3. **Informa,** facilitando a la persona interesada, la que te entrega sus datos, toda la información necesaria, incluyendo la posibilidad de ejercer sus *derechos*[2]*.*
4. **Recaba el consentimiento explícito**[3] de las personas interesadas.
5. **Asume la responsabilidad** del cuidado de las personas a las que solicitas los datos: ponte en contacto con el DPD de tu centro, para realizar un *análisis de los riesgos* del tratamiento de datos personales y, en caso necesario, una *evaluación de impacto* con su ayuda.

---

[1] La recogida, la guarda, la utilización, la conservación e incluso la cesión de los datos.

[2] Derechos ARSOPL.

[3] **Explícito:** el sujeto donante emite una declaración de consentimiento expresa (clara acción afirmativa) P.e. La firma de un documento o pulsar la acción «Acepto» en un entorno electrónico.

6. **Garantiza la seguridad** aplicando *medidas de seguridad* técnicas y medidas *organizativas* apropiadas, teniendo en cuenta los riesgos detectados, Sobre todo ello te asesorará el DPD de tu centro.

7. **Documenta con diligencia** con ayuda del delegado de protección de datos (DPD) de tu centro, para inscribir tu tratamiento en el Registro de actividades de tratamiento de la UPV/EHU o del centro donde investigues (1), para concretar cómo guardar los consentimientos firmados (2), para documentar el ejercicio de derechos de los interesados en coordinación con él (3), para hacer el análisis de riesgos y, en su caso, la evaluación de impacto (4), para la gestión de los incidentes (5), para recopilar los compromisos firmados de confidencialidad (6) y en caso necesario, los contratos de encargados de tratamiento (7).

Los siete pasos de la protección de datos en investigación con seres humanos

PASO 1. Identifica diez aspectos básicos:

1. Si son datos personales.
2. La finalidad que quieres darles.
3. De dónde y cómo los vas a recoger.
4. Las personas interesadas, reclutadas o donantes.
5. Si son datos especiales.
6. Los tratamientos que vas a realizar: archivar, ordenar, analizar, conservar, etc.
7. Los responsables de esta faceta del proyecto: Institución donde investigas, IP o persona delegada.
8. Las posibles cesiones a terceros.
9. Las posibles transferencias internacionales.
10. PONTE EN CONTACTO CON TU DELEGADA O DELEGADO DE PROTECCIÓN DE DATOS.

PASO 2. Actúa con licitud. Haz que el tratamiento sea legítimo.

PASO 3. Informa. Facilita a la persona que te entrega sus datos toda la información necesaria y la posibilidad del ejercicio de sus derechos.

PASO 4. Recaba el consentimiento explícito de las personas que donan sus datos.

PASO 5. Asume la responsabilidad del cuidado de las personas a las que solicitas los datos: ponte en contacto con el DPD de tu centro, para realizar un *análisis de los riesgos* del tratamiento de datos personales y, en caso necesario, una *evaluación de impacto* con su ayuda.

PASO 6. Garantiza la seguridad aplicando *medidas de seguridad* técnicas y medidas *organizativas* apropiadas, teniendo en cuenta los riesgos detectados, asesorado por tu DPD.

PASO 7. Documenta con ayuda de tu DPD para:

1. Inscribe tu tratamiento en el Registro de actividades del centro donde investigues.
2. Concreta cómo guardar los consentimientos firmados de las personas donantes.
3. Deja preparado el mecanismo de ejercicio de sus derechos ARSOPL.
4. Haz con tu DPD un buen análisis de riesgos y, en su caso, una evaluación de impacto.
5. Prevé la gestión de posibles incidentes.
6. Recopila los compromisos firmados de confidencialidad.
7. Recoge los contratos de encargados de tratamiento (si los hay).

1. Identifica

Reflexiona y proyecta (1) si son datos personales, (2) la finalidad que quieres darles, (3) su procedencia, (4) las personas interesadas (reclutadas/donantes), (5) si son datos especiales, (6) los tratamientos que vas a realizarles (7) la persona encargada de ello (8) las posibles cesiones a terceros y (9) las posibles transferencias internacionales. (10) Ponte en contacto con el DPD de tu centro.

Datos personales

Dato personal es cualquier *información* numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo sobre personas físicas identificadas o identificables. Las informaciones que hacen identificable a alguien son aquellas sobre su identidad física, fisiológica, económica, cultural, política, educativa, religiosa, etc. que permiten saber quién es la persona de la que procede la información.

Dato personal: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo sobre personas físicas identificadas o identificables.

Finalidad y procedencia

Has de tener muy claro al diseñar la futura investigación *por qué* y *para qué* recoges los datos, los registras, los estudias, los conservas, etc. y también que no puedes tratarlos posteriormente de manera incompatible con dichos fines, puesto que los datos personales siempre tienen que ser tratados con fines concretos, explícitos y legítimos.

También debes tener en cuenta *el criterio o principio de minimización* de datos: sólo debes recoger los datos imprescindibles para llevar a cabo la investigación, pero no recojas datos no contemplados en el diseño inicial del proyecto o «por si acaso hacen falta más adelante».

Lógicamente también necesitas prever y dejar constancia en tu proyecto de dónde extraerás esa información (directamente de la persona donante, documentos tipo historia clínica, informes u otras fuentes indirectas).

LAS 5 W SOBRE FINALIDADES Y PROCEDENCIAS

WHAT/qué: Describe con precisión la información o tipo de datos que necesitas recoger.

Principio de minimización de datos: sólo se recogen los datos imprescindibles.

WHY/por qué: Expón claramente con qué fines los recoges, registras, estudias, analizas, cruzas, conservas, etc.

Límites de la finalidad: no puedes tratarlos posteriormente de manera incompatible con esos fines.

WHERE/dónde: Especifica de dónde los recoges; si directamente de donante, de documentos tipo historia clínica, informes, expedientes o de otras fuentes indirectas y si será por medio de entrevistas, encuestas, test, fichas, etc. *Confidencialidad.*

WHO/quién: Recoge qué perfil de personas voluntarias serán donantes y quienes haréis cada tratamiento.

Consentimiento informado

WHEN/cuándo: Ordena los tiempos de cada paso: recogida, *pseudonimización*, conservación, trasferencia, etc.

Categoría de personas interesadas

La legislación llama «personas interesadas» a aquellas que te dan información propia que trasformarás en datos para tu actividad de investigación.

En realidad, son las *personas reclutadas* o *donantes* para la actividad de investigación aquellas a las que, una vez que les has explicado para qué las necesitas, con qué fines y en qué manera utilizarás y protegerás sus datos, te ceden esa información que les has solicitado.

Categorías especiales de datos

Hay datos, que puedes necesitar para la investigación y, que por su relevancia para la privacidad de las personas donantes tienes que tratar con mayor cuidado, y cumpliendo una serie de requisitos.

No todos los datos de carácter personal son iguales y la normativa los clasifica de la siguiente manera:

Datos sensibles, o especialmente protegidos

Categoría de datos que, debido a *su incidencia especial en la intimidad, las libertades públicas y los derechos fundamentales de la persona donante*, hace necesario que establezcas una mayor protección que con el resto de los datos personales (RGPD art. 9 y considerandos 51-56):

- Ideología u opiniones políticas.
- Afiliación sindical.
- Religión u opiniones religiosas.
- Creencias o creencias filosóficas.
- Origen racial o étnico.
- Datos relativos a la salud[1].
- Vida sexual u orientación sexual.
- Violencia de género y malos tratos.

- Datos genéticos[2].
- Datos biométricos[3].
- Datos relativos a condenas y delitos penales.
- Datos relativos a sanciones administrativas.

En las actividades de investigación universitarias y de otros centros es frecuente utilizar todo tipo de datos sensibles, dado que se investiga en ciencias biológicas, biomédicas, técnicas, sociales, jurídicas y de la conducta. Pero son especialmente delicados:

[1] **Datos relativos a la salud.** Todos aquellos que revelan información sobre el estado de salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria. De hecho, son datos de salud las informaciones relativas a enfermedad, discapacidad, riesgo de padecer enfermedades, tratamientos clínicos, estado fisiológico o biomédico, etc., independientemente de que la fuente sea su historia clínica o un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica *in vitro,* o incluso información transmitida por el propio participante en la actividad de investigación.

Ten en cuenta siempre que, para los tratamientos de recogida, uso, conservación, etc. que vayas a hacer de esta información, la normativa en protección de datos se complementa, entre otras muchas, con la *Ley de Autonomía del Paciente 41/2002*, que regula los derechos y obligaciones en materia de información y documentación clínica y que incluyen comunicación, toma de decisiones, consentimiento informado, acceso a la historia clínica, etc.

[2] **Datos genéticos.** Datos específicos de salud que identifican la información sobre las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos u otros análisis científicos.

[3] **Datos biométricos.** Informaciones sobre las características físicas, fisiológicas o conductuales de una persona, obtenidas con técnicas específicas como imágenes faciales, datos dactiloscópicos, etc. que permiten o confirman la identificación única de dicha persona (RGPD. art. 4.14).

Datos de menores

En principio no son datos sensibles, pero en la normativa se enuncia que debido a su *condición de vulnerabilidad* tienes que tratarlos como tales, ya que estas personas pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes a la recogida y la utilización de sus datos y es responsabilidad tuya evitar que sean vulnerados.

A modo orientativo considera que si los datos que vas a solicitar pueden generar al menor alguna tensión grave o afectación se consideraría una investigación invasiva y tendrás que pedir consentimiento a los representantes legales (padres o tutores) y asegurarte de que a partir de los 12 años el menor asiente. Cuando los datos no son de ese tipo solo necesitarás la autorización de los representantes legales en los menores de 14 años, a partir de esta edad son ellos los que autorizan o no. El DPD y el comité de ética que evalúe tu proyecto puede orientarte sobre las dudas que te surjan porque la casuística es muy variada y la ley no es taxativa en esta cuestión.

Tipo de investigación	Edad	Consentimiento
Investigación invasiva con datos	Menores de 18 años	Consienten los representantes legales. El mayor de 12 años asiente.
Investigación no invasiva con datos	Menores de 14 años	Consienten los representantes legales. El mayor de 12 asiente.

Datos de personas de colectivos en situación de especial vulnerabilidad

Es preciso que tengas un cuidado especial si la actividad de investigación implica el uso de datos de personas de colectivos en situación de especial vulnerabilidad, como menores (ya citados), discapacitados, ancianos, personas con riesgo de exclusión social, personas en situaciones políticas comprometidas, sin papeles, etc.

DATOS SENSIBLES, O ESPECIALMENTE PROTEGIDOS

Ideología u opiniones políticas
Afiliación sindical
Religión u opiniones religiosas
Creencias o creencias filosóficas
Origen racial o étnico
Datos relativos a la salud
Vida u orientación sexuales
Violencia de género y malos tratos
Datos genéticos
Datos biométricos
Datos relativos a condenas y delitos penales
Datos relativos a sanciones administrativas

Es bastante frecuente utilizar datos con especial incidencia en la intimidad, las libertades públicas y los derechos fundamentales de la persona donante pues se investiga en ciencias biológicas, biomédicas, técnicas, sociales, jurídicas y de la conducta.

Tratamiento de datos

Se denomina «tratamiento de datos» a cualquier operación o conjunto de operaciones que realices sobre información personal trasformada en dato o en conjunto de datos personales o que, no siendo personales, su agrupación identifica a una persona, ya sea por procedimientos automatizados o no. Así son tratamientos de datos la recogida, registro, organización, estructuración, conservación, adapta-

ción o modificación, extracción, consulta, utilización, comunicación por transmisión, su difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción de dichos datos.

En una actividad de investigación puedes tener que incluir uno o varios tratamientos de datos personales. De hecho, siempre vas a tener que «tratar» la información sobre los miembros de tu propio equipo investigador (datos personales) y en ocasiones, la de personas cuyos datos necesitas para llevar adelante la investigación.

TRATAMIENTO DE DATOS

Cualquier operación o conjunto de ellas con datos, por procedimientos automatizados o no, como:

- Recogida.
- Registro.
- Organización.
- Estructuración.
- Conservación.
- Adaptación.
- Modificación.
- Pseudonimización.
- Anonimización.
- Extracción.
- Consulta.
- Utilización.
- Transmisión.
- Difusión.
- Habilitación de acceso.
- Cotejo.
- Interconexión.
- Limitación.
- Supresión.
- Destrucción.
- Etc.

Son ejemplos de tratamiento de datos la gestión de la información (recogida, archivo y utilización) sobre las personas investigadoras, aunque este no es un tratamiento de datos para la investigación, la gestión de la información solicitada a los participantes (recogida, archivo y utilización), la seudonimización, codificación o disociación, la conservación de los documentos escritos de consentimiento informado, etc.

Este término puede llevarte a confusión porque el tratamiento de datos en una actividad de investigación suele referirse al *método estadístico o de análisis* empleado para extraer conclusiones a partir de los datos obtenidos en los experimentos, realizados en el laboratorio, en las muestras, en los trabajos de campo o en cualquier otro ámbito en el que se esté aplicando la metodología propia de cada actividad científica.

Responsable de tratamiento

Como su nombre indica es la persona física o jurídica que se responsabiliza del tratamiento o tratamientos de los datos, y que tiene que estar siempre identificada como tal en toda investigación.

Por ejemplo, la UPV/EHU es responsable de todos los tratamientos de investigación consignados en su registro de actividades de tratamiento (RAT). De hecho, **la persona investigadora principal, tutora o directora de tesis**, TFMs, TFGs, **tiene la consideración de responsable interna del tratamiento** a efectos prácticos, pero es siempre la UPV/EHU la responsable de todos los tratamientos con datos personales que tienen lugar en la institución universitaria.

Cuando, como responsable de la investigación, necesites los servicios de una persona o de una empresa que trate los datos personales bajo tus instrucciones, como por ejemplo, una empresa de servicios informáticos, es obligatorio que la institución, en nuestro caso la UPV/EHU firme un *Contrato de encargado de tratamiento* con dicha persona física o jurídica.

Cesión o comunicación de datos

Si tienes que ceder datos de carácter personal a terceros ajenos a la investigación (los terceros son aquellos que NO son ni las personas interesados, ni las personas investigadoras autorizadas, ni las personas encargadas de tratamiento) es obligatorio que obtengas el *consentimiento expreso y escrito* de la persona que te los donó.

Hay una situación especial que debes considerar: si la información que vas a comunicar a terceras personas incluye datos obtenidos del sujeto de investigación o persona donante, que revelan o pueden revelar *información de carácter personal de sus familiares*, la cesión requerirá también el consentimiento expreso y escrito de todos ellos.

Transferencias internacionales de datos

La transferencia internacional de datos consiste en la transmisión de datos de carácter personal fuera de la Unión Europea. Tanto tú como investigador como la institución en la que investigas, que es responsable del tratamiento, seréis exportadores porque estáis en territorio europeo y vais a realizar esa transferencia internacional.

Sólo puedes realizar transferencias de los datos personales de la investigación a un país u organización internacional si garantizan un nivel de protección adecuado de acuerdo con las condiciones establecidas en el capítulo V del RGPD. Cuando los datos vayan a ser transferidos fuera de la CE a algún país, territorio o sector específico de ese tercer país u organización internacional que la Comisión Europea no haya considerado que garanticen un nivel de protección adecuado, debe darse alguna o algunas de las circunstancias recogidas en el mencionado capítulo —cuya extensión casuística excede las pretensiones de esta guía— que autoricen dicha transferencia. Consulta el capítulo V o mejor consulta con el DPD de tu centro.

Si los datos personales de la investigación vas a albergarlos en la «nube» *(Cloud Computing)* es importante que tengas en cuenta que muchas de las empresas que prestan dichos servicios están ubicadas fuera de la Unión Europea y no proporcionan las garantías jurídicas adecuadas. En este caso recuerda que es imprescindible que hagas la consulta a tu DPD que podrá recabar esa información.

Delegada o delegado de protección de datos (DPD)

> Quien actúa como Delegado de Protección de Datos debe ser un solucionador de todas las situaciones relacionadas con el tratamiento de datos personales que se le planteen. No es responsable ni encargado del tratamiento de los datos, porque asumir tales tareas comprometería su neutralidad, pero es una figura que tiene un papel central en las organizaciones en las que se tratan categorías especiales de datos personales (Sánchez Ors, 2019)

La Delegada de Protección de Datos (DPD) —*en inglés, Data Protection Officer (DPO)*— es una persona especialista en protección de datos que las Universidades públicas y privadas y otras instituciones están obligadas a designar. Esta DPD se encarga de informar, asesorar, ayudar y responder a todas las consultas sobre protección de datos de la entidad responsable (en nuestro caso la UPV/EHU) y también del responsable interno del tratamiento (en nuestro caso el IP o la persona designada por el equipo investigador).

La DPD tiene que asegurase de que se cumplan las obligaciones legales en materia de protección de datos, también velando y cooperando con las autoridades de control (agencias española y vasca de protección de datos AEPD y AVPD).

Como investigador has de ponerte en contacto con esta persona para todo lo relacionado con el tratamiento de datos personales en tu investigación, ya que entre sus funciones están:

1. Informarte y asesorarte.
2. Ayudarte y supervisar los análisis de riesgo, las evaluaciones de impacto y el cumplimiento de su aplicación en los diferentes proyectos de investigación.
3. Controlar, coordinar y verificar las medidas de seguridad aplicables en el caso de tu investigación.

La DPD además siempre es miembro del Comité de ética en la investigación (CEI) que informará sobre tu proyecto, por lo que la relación entre tus tareas de investigación con datos personales y su trabajo como DPD es obligada, directa y constante.

DELEGADA O DELEGADO DE PROTECCIÓN DE DATOS (DPD)

La relación entre tus tareas de investigación con datos personales y su trabajo como DPD es obligada, directa y constante.

- Informa, forma y asesora.
- Ayuda y supervisa análisis de riesgo, evaluaciones de impacto y el cumplimiento de su aplicación.
- Controla, coordina y verifica las medidas de seguridad aplicables.
- Supervisa la gestión de las incidencias.
- Es referente para donantes sobre la información sobre protección de datos y ejercicio de derechos.
- Supervisa la organización de la información y documentación sobre protección de datos de la institución.
- Es miembro de los comités de ética en la investigación (CEI) que informan sobre los aspectos metodológicos, éticos y jurídicos de los proyectos de investigación.
- Es el nexo con las agencias autonómicas y nacional de protección de datos.

2. Actúa con licitud

Quiere decir sencillamente que cumplas con las condiciones para que el tratamiento de los datos personales en tu investigación sea legítimo (bien hecho y legalmente seguro).

Licitud del tratamiento

También llamada «base jurídica» que te permite usar datos en tu actividad de investigación: una vez que has identificado los datos que vas a recoger, de quiénes y el tratamiento que vas a darles, solo será legítimo que lo hagas si tienes el *consentimiento informado* de las personas donantes, que han de otorgar el consentimiento de manera libre, específica, explícita e inequívoca para todos los fines que vayas a utilizarlos (art. 6.1,2).

Otras bases jurídicas para el tratamiento de datos como son la *obligación legal*, el *interés público* o el *ejercicio de poderes públicos,* en el ámbito de la investigación con seres humanos no restan valor ni sustituyen al deber de información y de consentimiento que tienes, solo reflejan algunas situaciones en las que la persona donante conoce que existe un interés público (art. 8 LOPD y art. 9 REGPD).

Condiciones generales y requisitos para legitimar el tratamiento de datos sensibles

Aunque por regla general se prohíbe su recogida, su uso o guardarlos, es decir, el tratamiento de datos sensibles o especialmente protegidos descritos en el apartado anterior, puedes tratar datos sensibles para tu investigación si cumples una o más de las condiciones siguientes:

- Tienes el *consentimiento explícito* del interesado/donante para una *finalidad de actividad de investigación específica*.
- Son datos necesarios con fines de archivo e interés público, *fines de investigación científica o histórica o fines estadísticos* y están *seudonimizados* por otros.
- Hay razones de *interés público en el ámbito de la salud pública.*

Y tienes que cumplir los siguientes requisitos:

a) Obtén el *consentimiento explícito* por escrito de las personas reclutadas que confirme que acceden a darte sus datos, para qué servirán y cómo se tratarán.
b) Asegúrate de la calidad de esa información, es decir que son datos *adecuados, veraces y pertinentes* para tu investigación, ponderando la necesidad de los mismos. Es decir, valorando si todos los que vas a recoger son realmente indispensables para llevar a cabo la actividad de investigación. Si no son necesarios para la realización de la actividad de investigación, no hay que pedir esos datos personales (criterio o principio de minimización de datos).
c) Asegúrate también de que la recogida no se hace de forma desleal, fraudulenta o ilícita.
d) No olvides que en el caso de que recojas datos de salud para tu investigación, debes facilitar cualquier información que obtengas relacionada con la salud del donante que le sea útil.
e) Realiza un *juicio de proporcionalidad* entre la finalidad científica que persigues y el medio que vas a utilizar.

f) Cuando necesites para tu investigación datos de salud procedentes de la historia clínica de la persona interesada (donante) recoge siempre una hoja o *documento de información* y consentimiento que incluya:

- Nombre del profesional y del centro donde ha sido atendido el paciente.
- Propósitos de la petición.
- Expresa conformidad de publicación del caso clínico en publicaciones científicas dirigidas a profesionales de la salud.
- Nombre del paciente.
- Documento de identidad o pasaporte y su firma autorizando expresamente que se utilicen los datos de su historia clínica en las condiciones que se describen en el informe.

g) Asegúrate del cumplimiento del *compromiso de confidencialidad* por parte de las personas que tienen acceso a los datos, incluso cuando la relación que vincule a las partes haya finalizado.

> Código Penal, art 199: 1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.
>
> 2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

En este caso, como en otros, la casuística tan variada que aporta la investigación y la imprecisión de la ley, que no se hizo pensando en la investigación únicamente, hacen que sea imprescindible la orientación que pueda hacerte tu DPD y el comité de ética de la investigación de tu centro que sabrán ponderar con prudencia y de manera práctica estas cuestiones.

Circunstancias especiales de uso legítimo en investigación en salud

En las investigaciones relacionadas con la salud, especialmente en biomedicina, hay dos circunstancias especiales en las que podrás utilizar los datos personales con legitimidad:

1. Cuando la finalidad o el área de investigación esté relacionada con aquella para la que se obtuvo el consentimiento de la persona interesada; por ejemplo, el consentimiento lo prestó para el tratamiento de datos de investigación de un determinado tipo de cáncer y los quieres seguir tratando para investigación oncológica general. Tienes que *informar a los afectados* y necesitas un *informe previo favorable del Comité de Ética de Investigación.*
2. Los datos han sido *seudonimizados* por otro equipo con el consentimiento de las personas reclutadas para dicho tratamiento. El DPD te ayudará para que te asegures del *compromiso de confidencialidad* y de que *no se producirá la reidentificación.*

(Ver la Disposición adicional decimoséptima de la Ley Orgánica 3/2018 de Protección de datos personales y garantía de los derechos digitales, en adelante LOPD-GDD.)

3. Informa

Facilita a quien vaya a solicitar datos para tu investigación, toda la información necesaria, incluyendo la posibilidad de ejercer sus derechos, con un lenguaje claro y sencillo**,** de forma concisa, transparente, inteligible y de fácil acceso.

Quién tiene que informar y cuándo

La obligación de informar a las personas donantes sobre los aspectos referentes al tratamiento de sus datos corresponde a la persona *responsable* interna de la actividad de investigación (IP o a la designada por ella), que tiene que informar en nombre de la institución, en nombre de la UPV/EHU en nuestro caso.

Lógicamente, siempre tienes que poner toda la información a disposición de los posibles donantes con anterioridad a la recogida de los datos.

Excepciones a la obligación de informar

No es necesario que informes cuando:

- La persona donante ya disponga de la información.
- Es *imposible* informar o supone un *esfuerzo desproporcionado*, pero en tal caso tendrás que tomar medidas adecuadas y concretas para proteger sus derechos.

Cómo informar

Para informar correctamente debes adaptar adecuadamente la información al modelo de recogida de datos que vayas a utilizar y a sus características que serán variables en extensión, espacio, claridad, posibilidad de relacionar informaciones, etc.:

- Formularios en papel.
- Formularios en la web.
- Entrevista telefónica o presencial.

Recuerda que el cumplimiento diligente de la protección de datos te obliga a guardar un justificante de que has informado, y por ello es aconsejable que suministres la *información de primer nivel* o primera capa por escrito en el *Documento de consentimiento*, para que firme su recepción, y siempre con el link de acceso a la información completa o de segunda capa. El siguiente apartado explica en qué consiste la información en dos capas.

Muy importante: a menudo estarás solicitándole que participe en tu actividad de investigación (te apoyas en el *Documento de consentimiento informado para participación en investigación*) y a la vez que acceda a donarte determinados datos (*Documento de consentimiento informado para recogida, uso y conservación de datos* para dicha actividad de investigación). Incluso puedes tener que pedirle el consentimiento informado para otras cuestiones relacionadas con la misma actividad de investigación (por ejemplo, el consentimiento informado para toma de muestras u otras).

Reflexiona, imagina y organiza con una *visión integral*, las informaciones y la recogida de los consentimientos que requieres para tu actividad de investigación, de manera que la persona interesada no quede abrumada o confusa.

Las características de una buena información siempre son la sencillez, la claridad, la concisión, la transparencia, la inteligibilidad y el fácil acceso.

Presentación de la información por capas o niveles

La LOPD-GDD introduce este concepto de información por capas o niveles, refiriéndose a cómo presentar la información a la persona a la que solicitas los datos.

En un *primer nivel* le informas:

- de forma resumida
- en el mismo momento
- en el mismo medio en el que vas a recoger los datos.

Después puedes remitirle más información adicional en un *segundo nivel*:

- con una presentación más detallada de las informaciones
- usando el medio que consideres más adecuado para su presentación, comprensión y, si lo deseas, para su archivo.

Ejemplo: un documento en papel de solicitud de consentimiento informado (CI) para participar en la investigación, que incluya el consentimiento informado para la donación de datos necesarios para la investigación, recoge la *primera capa* de información y ese mismo documento en papel incluyes un enlace a la web donde está la *segunda capa* de información (anexo sobre Documento CI).

Primera capa o primer nivel de información

El contenido básico de la información que das a la persona donante se corresponde con la llamada «primera capa» o «primer nivel de información» en la norma y es lo que deben saber las posibles donantes, para decidir *si acceden o no* a cederte sus datos:

1. Código del tratamiento (código que figura en el Registro de Actividades de Tratamiento RAT).
2. Nombre del tratamiento.

3. Responsable del tratamiento (institución: UPV/EHU en nuestro caso).
4. Procedencia de los datos cuando no proceden de la persona donante.
5. Finalidad del tratamiento de datos.
6. Legitimación del tratamiento de datos.
7. Destinatarios de cesiones y transferencias internacionales de datos.
8. Derechos (acceso, rectificación, supresión, oposición, portabilidad y limitación ARSOPL).

Esta información te la proporcionará el Delegado de Protección de Datos cuando registre su tratamiento en el RAT.

Segunda capa o segundo nivel información

Es ese segundo nivel de detalle incluirás la siguiente información:

1. Código del tratamiento (código que figura en el Registro de Actividades de Tratamiento RAT).
2. Nombre del tratamiento.
3. Responsable del tratamiento: datos de contacto de la UPV/EHU y del Delegado de Protección de Datos.
4. Procedencia de los datos cuando no proceden de la persona donante (ampliado).
5. Finalidad del tratamiento de datos.
6. Periodo de conservación de los datos.
7. Legitimación del tratamiento de datos.
8. Destinatarios de cesiones y transferencias internacionales de datos.

9. Datos de carácter personal del tratamiento (relación exhaustiva de los datos que serán tratados en la investigación).
10. Derechos y manera de ejercerlos (acceso, rectificación, supresión, oposición, portabilidad y limitación (ARSOPL).
11. Información adicional (enlace a la página web sobre protección de datos personales de la UPV/EHU.

Esta información te la proporcionará el Delegado de Protección de Datos cuando registre tu tratamiento en el RAT.

INFORMACIÓN PARA LA PERSONA A LA QUE SOLICITAS LOS DATOS

Contenido

- Veraz y suficientemente extenso, preciso, claro y comprensible.
- Se aconseja suministrar toda la *información de primer nivel o capa* por escrito en el *Documento de consentimiento.*
- Pon siempre el enlace de acceso a la información completa o de segunda capa.

Forma

- Adapta la información al modelo de recogida de datos:
  - — Formularios en papel.
  - — Formularios en la web.
  - — Entrevista telefónica o presencial.
- Incluye en el mismo documento de consentimiento, si es posible, la información sobre la investigación en la que le pides participación y sobre los datos que le solicitas para ella y las dos solicitudes de consentimiento.

Custodia

- Guarda, en el soporte más apropiado, el justificante de que has informado y ha consentido.

Recomendación del CEISH UPV/EHU (Comité de Ética de Investigación con Seres Humanos) sobre cómo informar

Presentar la información básica (primera capa) y remitir a la información completa del tratamiento en el RAT público de la UPV/EHU (segunda capa) es una opción legal. No obstante, el CEISH UPV/EHU recomienda poner la siguiente cláusula en el documento de consentimiento informado —debidamente adaptada a cada investigación— bajo un epígrafe que diga *Información sobre protección de datos:*

- Se le informa de que de conformidad al Reglamento Europeo de Protección de Datos (UE2016/679):
- El código del tratamiento de datos es: . . . . . .
- El nombre del tratamiento de datos es: . . . . . .
- La finalidad de este tratamiento es: . . . . . .
- El responsable del tratamiento de datos es la UPV/EHU:

Identidad: Universidad del País Vasco/EuskalHerriko Unibertsitatea

CIF: Q4818001B

Dirección postal: Barrio Sarriena, s/n, 48940-Leioa (Bizkaia)

Página web: www.ehu.eus

Datos de contacto del Delegado de Protección de Datos: dpd@ehu.eus

- Los datos personales que se le solicitan son: . . . . . .
- El periodo de conservación de sus datos será: Los datos se conservarán mientras no se solicite su supresión por la persona interesada y, en cualquier caso, siempre que estén abiertos los plazos de recurso y/o reclamación procedente o mientras sigan respondiendo a la finalidad para la que fueron obtenidos.
- La legitimación del tratamiento es: su consentimiento informado (u otras fuentes de legitimación si fuera el caso).

- Cesiones: (Indicar las cesiones o en caso de no haberlas anotar «No se cederán datos salvo previsión legal»).
- Transferencias internacionales de sus datos: (Indicar las transferencias o en caso de no haberlas anotar «No se efectuarán transferencias internacionales»).
- Los derechos sobre sus datos son los de acceso, supresión, rectificación, oposición, limitación del tratamiento, portabilidad y olvido. Puede ejercerlos enviando su petición a dpd@ehu.eus
- Tiene a su disposición información adicional en http://www.ehu.eus/babestu
- La información completa sobre este tratamiento está en: https://www.ehu.eus/es/web/idazkaritza-nagusia/ikerketa-datu-pertsonalen-tratamenduak

Si consideras que la información sobre protección de datos así presentada resulta farragosa o de difícil comprensión para las personas participantes en la investigación, puedes intentar adaptarla a su perfil, pero ten en cuenta que es obligatorio informar de todos los extremos que aparecen en la información básica (primera capa).

Información sobre los derechos de Acceso, Rectificación, Supresión, Oposición, Portabilidad y Limitación (ARSOPL)

Con esta información sobre los derechos siempre se trata de promover la *capacidad de decisión y de control* sobre los propios datos personales. Por ello, como responsable de la investigación, tienes que informar a la persona donante sobre sus derechos, sobre cómo puede ejercerlos y sobre la forma de ponerse en contacto para hacerlo:

- Derecho de **A**cceso o derecho a solicitar información al responsable sobre si sus datos están siendo tratados y en caso afirmativo qué datos son.
- Derecho de **R**ectificación o derecho a solicitar la modificación de datos que sean inexactos o incompletos.

- Derecho de **S**upresión o derecho a solicitar la supresión de los datos en determinados supuestos, pero no se suprimirán los resultados ya obtenidos.
- Derecho de **O**posición o derecho a oponerse al tratamiento de sus datos personales por motivos relacionados con su situación particular.
- Derecho a la **P**ortabilidad de los datos o derecho a solicitar que se le faciliten los datos en un formato estructurado, de uso común y lectura mecánica y el derecho a transmitirlos a otro responsable.
- Derecho a la **L**imitación del tratamiento o derecho a solicitar que se limite el tratamiento de sus datos en determinadas condiciones.

PROMOVER LA CAPACIDAD DE DECISIÓN
Y DE CONTROL SOBRE LOS PROPIOS DATOS PERSONALES
DERECHOS ARSOPL

DERECHO DE ACCESO: a que se le informe sobre si sus datos y cuales están siendo tratados.

DERECHO DE RECTIFICACIÓN: a que se modifiquen los datos que sean inexactos o incompletos.

DERECHO DE SUPRESIÓN: a que se eliminen los datos en determinados supuestos. No se suprimirán los resultados ya obtenidos.

DERECHO DE OPOSICIÓN: a que no se traten sus datos por motivos relacionados con su situación particular.

DERECHO A LA PORTABILIDAD: a que se le faciliten los datos en un formato estructurado, de uso común y lectura mecánica y a ejercer su derecho a transmitirlos a otro responsable.

DERECHO A LA LIMITACIÓN DEL TRATAMIENTO: a que se limite el tratamiento de sus datos en determinadas condiciones.

Como responsables de la investigación, institución e IP están obligadas informar a la persona donante sobre estos derechos, cómo puede ejercerlos y la forma de contactar para hacerlo.

Información sobre el tiempo de conservación

Al informar sobre el tiempo de conservación en el CI, tienes que indicar al posible donante que el plazo mínimo de conservación es de *cinco años*, con fines de auditoría y verificación de la investigación realizada con esos datos. También le informarás de que puedes conservar los datos recogidos para la investigación mientras no solicite su *supresión* y esos datos sigan respondiendo a la finalidad para la que fueron obtenidos y de que no puede pedirte que suprimas los resultados obtenidos con sus datos hasta el momento de la solicitud de supresión.

Por último, recuerda que, si aplicas medidas técnicas apropiadas, como la anonimización, puedes conservarlos más tiempo.

TIEMPO DE CONSERVACIÓN DE LOS DATOS

- Plazo mínimo *CINCO AÑOS*, con fines de auditoría y verificación de la investigación.
- Se pueden conservar más tiempo para la investigación para la finalidad para la que se obtuvieron si no hay solicitud de *supresión.*
- No se puede pedir la supresión de los resultados obtenidos antes de ejercerse este derecho.
- Con medidas técnicas apropiadas (anonimización) se pueden conservar más tiempo.

Información sobre una posible cesión de datos

Para compartir, comunicar, dejar que otro acceda o traspasar datos de la persona donante a un tercero, dicha persona debe tener constancia de la posible cesión, ya que será quien te permita o no ese traspaso.

Lo más sencillo es que en el documento de CI, en el apartado de información sobre protección de datos, incluyas la *solicitud de cesión* con un espacio específico para la *recogida de su consentimiento*. Si no lo vas a hacer indícale que *no habrá cesión* en ningún caso. Se

entiende como cesión internacional cuando los datos se van a ceder fuera del territorio de la Unión Europea o a países que no garantizan un nivel de protección adecuado según la Comisión Europea.

* La comunicación de datos a un *encargado de tratamiento* (ver punto 1), con el que tienes firmado un contrato, no se considera una cesión de datos, ya que dicho encargado sólo tratará los datos conforme a tus instrucciones.

Tratamientos posteriores o usos adicionales de los datos

Se puede dar el caso de que, una vez informada la persona donante y habiendo aceptado, te plantees una nueva investigación con un nuevo tratamiento de datos compatible con el anterior. En ese caso, vas a tener que informarle por correo postal, por medios electrónicos u otros y necesitas un *Informe Favorable previo del Comité de Ética de Investigación*.

4. Recaba el consentimiento explícito

> «Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.» (RGPD. art. 4.11)

En la nueva regulación española hay una disposición específica (DA 17) sobre los Tratamientos *de datos de salud*, que son especialmente protegidos, que señala que, para investigar con ellos, precisas del consentimiento de los interesados, salvo que te los seudonimice alguien separado técnica y funcionalmente de tu equipo investigador. Es decir, regula que no es garantía suficiente que la seudonimización la hagáis tú o alguien de tu equipo investigador cuando no se cuenta con el consentimiento de la persona donante.

Las exigencias al respecto de los datos especiales en investigación en salud son exigibles también en otras áreas de investigación en tanto en cuanto se trata de datos de carácter especial (ciencias biológicas, biomédicas, sociales, jurídicas y de la conducta). La nueva regulación no ha cambiado esencialmente, pero es más exigente con el consentimiento expreso, ya que antes se aceptaba el consentimiento tácito, aunque ciertamente se refería sobre todo a situaciones de transacciones comerciales.

En resumen, la nueva legislación refuerza la necesidad del consentimiento como regla general, si bien ofrece, en caso de investigación en salud, la posibilidad de utilización de los datos seudonimizados por personas ajenas a la investigación. De todas formas, este es un aspecto que te ayudará a discernir prudencialmente tanto el DPD como el CEI de tu centro.

Características del consentimiento

El consentimiento de la persona donante de sus datos personales es la expresión libre de que acepta que trates información suya, sus datos, para una finalidad concreta, bajo unas determinadas condiciones de las cuales ha sido previamente informada.

EXPLÍCITO

LIBRE

INFORMADO

INEQUÍVOCO

ESPECÍFICO

VERIFICABLE

DISTINGUIBLE

MANIFIESTO

REVOCABLE

Actualmente existen todavía prácticas que se encuadraban en el llamado *consentimiento tácito,* pero debes saber que han dejado de ser aceptables: el silencio, la inacción o las casillas previamente seleccionadas como forma de recabar el consentimiento, como supuesta aceptación de la donación de datos ya no son válidas. Solo se considera bien hecho cuando es:

- *Explícito*: el sujeto donante emite una declaración de consentimiento expresa (siempre una clara acción afirmativa) P.e. La firma de un documento o pulsar la acción «Acepto» en un entorno electrónico.
- *Libre*: prestado en un marco de libertad, no puede estar condicionado a, por ejemplo, una rebaja en una tarea académica, la

consecución de un bien material, o a cualquier otro tipo de condición. Al evaluar si el consentimiento se ha dado libremente, siempre has de tener en cuenta la posible existencia de condiciones que limiten esa libertad de decisión.

- *Informado*: para que el consentimiento sea realmente informado, la persona posible donante debe saber y entender qué está decidiendo y para ello se lo has de explicar de manera comprensible, tal como se expone en el Cap. 3.
- *Inequívoco*: la información sobre la prestación de consentimiento para donarte sus datos debe estar muy clara y no mezclada con otras condiciones de la investigación o con solicitudes para donación de muestras, realización de encuestas, etc. (Ver en Cap. 3. «Cómo informar»).
- *Específico*: tienes que recabar el consentimiento para cada finalidad y explicar bien que no vas a usarlos para otros fines.
- *Verificable*: como responsable del tratamiento debes poder demostrar ante cualquier autoridad competente, persona o comité pertinente, que la persona donante te consintió el tratamiento de sus datos personales para los fines de tu investigación.
- *Distinguible y manifiesto*: si el consentimiento para la recogida, uso y conservación de sus datos te lo da la persona donante en el texto y en el contexto del consentimiento para participar en tu proyecto de investigación, tienes que presentársela de manera que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.
- *Revocable*: tiene que poder retirar el consentimiento en cualquier momento y has de informarle de que puede solicitarlo de manera sencilla sin consecuencias para ella y de cómo hacerlo.

Validez del consentimiento recabado antes de la entrada en vigor del RGPD

Si obtuviste el consentimiento antes de mayo de 2018 no tienes obligación de recabar de nuevo el consentimiento con las condiciones del RGPD, ya que cuando te lo dieron esa norma no era aplicable. Por diligencia y honradez se recomienda facilitar la nueva información, en la medida de lo posible.

Consentimiento recabado de forma electrónica

El consentimiento informado recabado de esta forma es tan válido como en papel y si no quieres tener documentación en papel y prefieres tener todo en formato electrónico, incluso puedes recogerlo con firma digital o con certificado electrónico. Recuerda que en todos los casos la persona donante debe realizar una clara acción afirmativa para que pueda considerarse válido su consentimiento y que has de mantener esos consentimientos, con los datos de los donantes, también protegidos.

La aceptación mediante un clic en una casilla, en que dejes expresamente la posibilidad de decidir si acepta o no el tratamiento de los datos, se considera un consentimiento válido siempre que NO lo hagas a través de casillas premarcadas.

Consentimiento prestado por menores de edad

La recogida, uso y conservación, es decir, el tratamiento de los datos personales de un menor requiere su consentimiento. El consentimiento prestado por mayores de 14 años se presupone válido y para los menores de 14 años es necesario que también autoricen sus padres o tutores. Recuerda que, si vas a recabar datos *on line* de menores, consulta a tu DPD, porque tienes que establecer procedimientos para que se pueda verificar el consentimiento parental.

5. Realiza un análisis de los riesgos del tratamiento de datos personales y, en caso necesario, una evaluación de impacto

Como investigador tienes que asumir tu responsabilidad aplicando un *nivel de seguridad adecuado* al riesgo que puede haber de que accedan a ellos personas no autorizadas, o de que los datos se alteren o se destruyan o de que no se pueda acceder a ellos.

Para ello, tienes dos herramientas: el análisis de riesgo y la evaluación de impacto. Para realizar estas tareas cuentas con el DPD de la UPV/EHU que te asesorará en ello.

INCIDENTES CON LOS DATOS	DAÑOS A LOS VALORES
Revelación a personas no autorizadas…	A la confidencialidad
Alteración, inexactitud, manipulación…	A la integridad
Pérdida, inaccesibilidad…	A la disponibilidad

Análisis de Riesgos (AR)

> El RGPD señala que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas. De acuerdo con este enfoque, algunas de las **medidas que** el RGPD establece **se aplicarán sólo cuando exista un alto riesgo** para los derechos **y** libertades, mientras que **otras** deberán modularse **en función del nivel y tipo de riesgo** que los tratamientos presenten. (AEPD)

Como señala la Agencia Española de Protección de Datos (AEPD), con la ayuda de tu DPD, tienes que analizar la naturaleza de tu investigación, el contexto en el que se desarrolla y su finalidad para saber los riesgos posibles de que un impacto negativo, sobre los datos personales que tratas, afecte a los derechos y libertades de las personas que te los han suministrado. Las tres propiedades de la información que has recogido que pueden verse afectadas por un incidente son:

1. **Confidencialidad:** propiedad de la información de no ser revelada a personas no autorizadas. Posible incidente: *revelación, robo…*
2. **Integridad:** propiedad de la información de no ser alterada y conservar su exactitud. Posible incidente: *alteración, manipulación…*
3. **Disponibilidad:** propiedad de la información de estar accesible para las personas autorizadas. Posible incidente: *inaccesibilidad, pérdida…*

El análisis de riesgos consiste en analizar las probabilidades de que, en un momento dado, pueda verse afectada alguna de esas tres propiedades. Te has de plantear la hipótesis de que personas no autorizadas accedan a los datos de tu investigación, que los datos sean manipulados indebidamente de forma accidental o deliberada, que no puedas acceder a los datos de la investigación por un incidente.

Tras imaginar esas posibilidades reales (riesgo bajo/riesgo alto), tienes que valorar qué daño (leve/grave) puede causar a los derechos de

las personas donantes si se producen y establecer unas medidas de seguridad (sencillas/complejas) en función del nivel y tipo de riesgo.

En la UPV/EHU el Análisis de Riesgos lo realizas con el DPD, antes del registro del tratamiento en el RAT de la institución, y tiene en cuenta las respuestas que das sobre medios utilizados en el tratamiento y medidas de seguridad aplicadas. Es importante que los equipos investigadores tengáis claro:

1. El análisis de escenarios concretos de posibles amenazas para la seguridad de los datos personales manejados en vuestra investigación. Por ejemplo, un consentimiento informado en papel que siempre contiene la firma de los participantes; su pérdida o uso ilegítimo puede facilitar la suplantación de su identidad en documentos legales de todo tipo. Otra fuente de incidentes es el envío de información con datos personales sin cifrar a otros miembros del equipo investigador.
2. El uso del equipamiento informático corporativo de la UPV/EHU que es el que incorpora medidas de seguridad «por defecto». Si esto no fuera posible, el equipamiento utilizado debe incorporar medidas de seguridad equivalentes al equipo suministrado por la institución.

Elaboración de una Evaluación de Impacto (EIPD)*

Si concluyes al hacer el Análisis de riesgos (AR) con tu DPD, que el tratamiento de datos que necesitas para la investigación conlleva un *riesgo significativo o alto* para los derechos de las personas, tendréis que realizar una *Evaluación de Impacto (EIPD)*. Es decir, un proceso sistemático con una metodología determinada para analizar los riesgos significativos que tu investigación puede comportar para la protección de los datos, los derechos y libertades de las personas que te los han donado. El DPD dispone habitualmente de un modelo o programa que permite realizar ese proceso sistemático.

La EIPD es una herramienta para situaciones de alto riesgo o para cuando utilizas grandes cantidades de datos especialmente protegidos (art. 35 RGPD).

El objetivo de la EIPD es determinar (a) la *probabilidad* de que se produzcan situaciones no deseadas, (b) la *gravedad* de sus consecuencias y (c) las *medidas de contención* que tenemos que tomar para evitar o paliar sus consecuencias.

De esta forma, puedes establecer el *Nivel de Riesgo Inicial* de las operaciones de recogida y uso de datos que has diseñado para llevar a cabo tu proyecto de investigación y el *Nivel de Riesgo Residual Aceptable* una vez llevadas a cabo las medidas de contención o seguridad.

Gracias a esta EIPD puedes concretar y describir las *medidas de seguridad o contención y los protocolos adecuados* que has previsto inicialmente para reducir, prevenir y corregir los riesgos (probabilidad y gravedad) en cada momento clave de la recogida, el uso y la conservación de los datos necesarios para tu investigación.

Recomendación u obligación de la EIPD: la EIPD no siempre es necesaria, pero es recomendable que, al plantearte cada nueva recogida y uso de datos, hagas con tu DPD, un Análisis de riesgos (AR) para determinar la conveniencia o no de realizar una EIPD.

La EIPD es OBLIGATORIA en las investigaciones de los siguientes tipos:

1. *Alto riesgo:* la recogida, uso y guarda pueden entrañar un alto riesgo para los derechos y libertades de las personas físicas. Ej. personas emigradas por razones de ideología o identidad sexual.
2. *Evaluación sistemática*: cuando, sistemáticamente, se recojan y evalúen aspectos personales de personas físicas basadas en un tratamiento automatizado. Ej. elaboración de perfiles.
3. *Uso de tecnologías invasivas de la privacidad:* en el proyecto de investigación se utilizarán:

    a) Aeronaves no tripuladas (drones).
    b) Minería de datos.
    c) Biometría.
    d) Técnicas genéticas.
    e) Geolocalización.
    f) Videovigilancia a gran escala.
    g) Vigilancia electrónica.

EVALUACIÓN DE IMPACTO OBLIGATORIA

Investigaciones de alto riesgo para los derechos y libertades de personas por la recogida, uso y guarda de sus datos. Ej. personas emigradas por razones de ideología o identidad sexual.

Investigaciones con evaluación sistemática de aspectos personales en un tratamiento automatizado. Ej. elaboración de perfiles.

Investigaciones son uso de tecnologías invasivas de la privacidad:

- Aeronaves no tripuladas (drones).
- Minería de datos.
- Biometría.
- Técnicas genéticas.
- Geolocalización.
- Videovigilancia a gran escala.
- Vigilancia electrónica.

Investigaciones con tratamiento a gran escala de datos especialmente protegidos.

Ej: con muchos datos, a muchas personas, en zonas geográficas amplias, con tecnologías invasivas de la privacidad, a menores y personas vulnerables.

4. *Tratamiento a gran escala de datos especialmente protegidos*, que serían por ejemplo investigaciones:
    - Que requieren de una gran cantidad de datos (volumen, variedad y duración o permanencia de la actividad de recogida, uso y guarda de datos).
    - En un ámbito geográfico regional o superior (extensión geográfica de la actividad de recogida, uso y guarda de datos).
    - Que afectan a gran número de personas (bien en términos absolutos, bien como proporción de una determinada población).

- Referidas a datos sensibles como biométricos, de salud, etc. y también que incluyan datos personales relativos a menores*.
- En las que se aplican nuevas tecnologías (que puedan tener riesgos para la privacidad) a esa gran escala.
- Que entrañan alto riesgo para los derechos y libertades de los interesados.

Contenidos de la EIPD[4]

El resultado final de la EIPD tiene que ser un *Informe de evaluación de impacto o* un *conjunto de documentación* que informe adecuadamente y recoja las características del tratamiento evaluado y de la gestión de los riesgos, es decir, de las decisiones tomadas para mitigarlos. Este informe, cuando lo haya, quedará recogido con el resto de la documentación en tu archivo de documentación sobre protección de datos en tu investigación concreta, que te ha proporcionado tu DPD.

Ese INFORME DE EVALUACIÓN DE IMPACTO tiene que incluir:

1. *Análisis del proyecto*: donde nuevamente se detallan las *categorías* de datos que recogerás, usarás y guardarás, las *personas* que podrán acceder a ellos, los *flujos* de información y las *tecnologías* utilizadas (cap. 1).
2. *Juicio de proporcionalidad*: en el que se discierne si la finalidad que persigues se puede conseguir por otros medios, por ejemplo, usando otros datos o menos datos, reduciendo el colectivo de personas donantes cuantitativa o cualitativamente, con otras tecnologías menos invasivas o aplicando otros procedimientos o medios de tratamiento, etc. Este juicio se asienta en tres aspectos a revisar que ya has trabajado en la primera fase (cap. 1):

[4] **Guía de la Agencia Española de Protección de datos.** La AEPD ha publicado en su web una guía para una Evaluación de Impacto en la Protección de Datos Personales. Se trata de un documento de gran ayuda para desarrollar una EIPD.

a) Idoneidad*:* los datos recogidos sirven para conseguir el objetivo propuesto con la investigación.
b) Necesidad*:* no existe otra forma más moderada para llevar a cabo la investigación con la misma eficacia.
c) Proporcionalidad*:* es ponderada o equilibrada, porque se derivan más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.

3. *Evaluación de los riesgos:* apartado donde analizas los posibles riesgos para la protección de datos de los afectados, que ya has confirmado en los puntos anteriores que necesitarás y valoras su probabilidad y el impacto de su materialización.

4. *Medidas previstas:* incluyes las medidas que vas a establecer, asesorado por tu DPD, para afrontarlos.

Como ves para realizar una buena EIPD y un adecuado *Informe EIDP* es imprescindible la colaboración del *Delegado de Protección de Datos* (DPD) dpd@ehu.eus , tanto con intervención activa en el diseño y ejecución de la evaluación, como en sus funciones de coordinación, interlocución principal o colaboración con la persona evaluadora.

Ten en cuenta que la obligatoriedad de hacer la EIPD es consecuencia de la naturaleza, la metodología y los medios utilizados en la investigación. En la UPV/EHU el formulario mediante el cual solicitas al Delegado de Protección de Datos el registro del tratamiento en el RAT de la UPV/EHU evalúa, en función de la información que aportas en el mismo, la necesidad de hacer una EIPD. Cuando bajo el nivel de impacto estimado del tratamiento aparece la frase «SE DEBE HACER UNA EVALUACIÓN DE IMPACTO PARA ESTE TRATAMIENTO» es obligatorio que respondas al apartado 16 de dicho formulario, que constituye en sí mismo una EIPD. Pero mejor aún que todo eso, es replantear aspectos éticos y metodológicos que permitan abordar la investigación con un menor nivel de impacto en la privacidad y los derechos de los participantes. Muchas veces no es posible, y es entonces cuando hay que replantearse sinceramente la pertinencia de la metodología pensada para la investigación frente al riesgo que supone para la privacidad y derechos de los donantes. Si la respuesta es afirmativa, su justificación constituye la EIPD y debe ser lo más razonada y minuciosa posible.

Recogida, uso y conservación *on line* (en la nube)

La utilización para la investigación de un tratamiento de datos *on line* como el *cloud computing* o computación en la nube, requiere que realices una buena evaluación y que adoptes las medidas adecuadas:

- Evaluar los *riesgos asociados* al tratar esos datos en la nube.
- Aplicar *medidas de minimización de riesgos* como la seudonimización o la anonimización, también si tratan Macrodatos o Big data[5].
- Recoger y evaluar las *condiciones del servicio en la nube*, su cumplimiento de los requisitos normativos (p.e. la ubicación física de los datos: si están en espacio «seguro» legalmente) y las medidas de seguridad (p.e. el cifrado de la información en tránsito *on line*).
- Firmar un *contrato con el prestador de servicios en la nube* (cuando no sea la universidad) ya que va a tener la consideración de «encargado de tratamiento», que incluya que cuando termine la prestación de servicios, los datos serán devueltos al responsable de la investigación que ha contratado el servicio.

[5] Big Data (Macrodatos): la gran cantidad de datos sobre nuestros hábitos, horarios, etc. recogidos a través de dispositivos (móviles, pulseras deportivas, relojes inteligentes, ordenadores, etc.) conforman el Big Data, a través del cual las empresas analizan conjuntos de datos, los datos pueden ser moldeados o probados, se buscan tendencias, se pueden detectar áreas problemáticas, etc. Normalmente, en el Big Data todos los datos se encuentran anonimizados, por lo que no se puede identificar a una persona en particular a través de esos datos, pero hay que implantar medidas de seguridad que se tienen aplicar para que la anonimización no sea reversible. **La anonimización de datos personales consiste en** acotar y eliminar la información concreta que nos permite identificar al afectado. El principal objetivo es evitar, de forma definitiva, que se le pueda volver a identificar cuando los datos sean reutilizados.

6. Garantiza la seguridad

El artículo 5.1.f (RGPD) determina la necesidad de que establezcas garantías de seguridad adecuadas que eviten, fundamentalmente:

- El tratamiento no autorizado o ilícito de los datos personales que has solicitado.
- La pérdida de esos datos personales, su destrucción o el daño accidental.
- La falta de disponibilidad de los datos.

Para que no ocurra, tienes que establecer unas medidas técnicas y organizativas que aseguren la integridad, la confidencialidad y la disponibilidad, pero que además te permitan demostrar, (cuando se requiera en supervisión o auditoría) que las estás llevando a la práctica durante y después de la investigación. Tu DPD te asesorará en todo ello.

Medidas de seguridad organizativas

Todas las personas de tu equipo de investigación han de saber que tienen un deber de confidencialidad que persiste cuando finalice la investigación y también que deben evitar el acceso de personas no autorizadas a los datos. Es conveniente que todos aquellos que vayan a tener acceso a los datos, firmen un documento de confidencialidad.

Para hacer efectivos esos deberes al diseñar del proyecto debes implantar las siguientes medidas organizativas:

1. Es conveniente adoptar unas *Normas de seguridad* para el tratamiento de los datos conocida por todo tu equipo investiga-

dor. En nuestro caso, dichas normas deben ser compatibles con la Política de Seguridad de la Información de la UPV/EHU (ACUERDO de 25 de abril de 2013, del Consejo de Gobierno de la UPV/EHU, por el que se aprueba la Política de Seguridad de la Información de la Universidad del País Vasco / Euskal Herriko Unibertsitatea (UPV/EHU)).

2. *Roles y responsabilidades*, especialmente quién va a ser la persona responsable de la seguridad.
3. *Gestión de los ordenadores*, del software, de los dispositivos de almacenamiento y de los recursos de red.
4. *Formación en medidas de seguridad cotidianas*:
   - No dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.).
   - Proceder antes de ausentarse al bloqueo de la pantalla o al cierre de la sesión; almacenar los documentos en papel y soportes electrónicos en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.
   - No comunicar datos o cualquier información personal a terceros, especialmente durante las consultas telefónicas, correos electrónicos, etc.
5. *Procedimientos seguros de acceso y respuesta* a la persona que ha donado sus datos cuando quiera ejercer sus derechos: medios electrónicos, remisión al IP, al DPD, dirección postal, etc.
6. *Protocolo de actuación ante una violación de la seguridad*: en caso de acceso indebido a los datos personales, una alteración de la información o una pérdida del acceso, debes ponerte en contacto de inmediato con tu DPD para registrar el incidente y evaluar sus consecuencias. Si la brecha de seguridad puede constituir un riesgo para los derechos y libertades de las personas físicas tienes que informarles a ellas sin dilación indebida y a la institución (UPV/EHU, en nuestro caso) a través del DPD, notificar a la Agencia Española de Protección de Datos en un máximo de 72 horas, incluyendo toda la información necesaria para esclarecer los hechos, a través de su sede electrónica https://sedeagpd.gob.es

MEDIDAS DE SEGURIDAD ORGANIZATIVAS PARA EL EQUIPO INVESTIGADOR

- Adoptad unas normas de seguridad del equipo para el tratamiento de los datos.
- Distribuid los roles: especialmente quién va a ser la persona responsable de la seguridad.
- Organizad la gestión de los ordenadores, del software, de los dispositivos de almacenamiento y de los recursos de red.
- Cumplid medidas de seguridad cotidianas:

    1. No dejar los datos personales expuestos a terceros en pantallas electrónicas desatendidas, en documentos en papel en zonas de acceso público, en soportes con datos personales, etc.
    2. Proceder antes de ausentarse al bloqueo de la pantalla o al cierre de la sesión.
    3. Almacenar siempre los documentos en papel y soportes electrónicos en lugares muy seguros.
    4. No comunicar datos o cualquier información personal a terceros, especialmente durante las consultas telefónicas, en correos electrónicos, etc.

- Estableced procedimientos seguros de acceso y respuesta a la persona que ha donado sus datos cuando quiera ejercer sus derechos: medios electrónicos, remisión al IP, al DPD, dirección postal, etc.
- Ante una violación de la seguridad por acceso indebido, alteración de la información o pérdida del acceso, poneos en contacto inmediatamente con vuestro DPD.

Medidas de seguridad técnicas

Las medidas técnicas son medidas de seguridad elementales para evitar riesgos o minimizarlos que tienen que ser revisadas periódicamente de manera automática (software o programas informáticos) o manual:

1. *Control de acceso y autentificación: perfiles y contraseñas:*

    a) Dispón de varios perfiles o usuarios distintos para cada finalidad: cuando utilicéis el mismo ordenador o dispositivo para el tratamiento de datos personales de la investigación y para otros fines de uso personal o profesional, se recomienda mantener separados dichos usos.

    b) Dispón de perfiles con derechos de administración para la instalación y configuración del sistema y perfiles de usuarios sin privilegios o derechos de administración para el acceso a los datos personales: esta medida evita que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.

    c) Garantiza la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos, con al menos 8 caracteres, mezcla de números y letras.

    d) Identificación inequívoca: cuando vayan a acceder distintas personas a los datos, dispón para cada una de un usuario y contraseña específicos.

    e) Contraseñas: debes garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso pueden compartir las contraseñas ni dejarlas anotadas en lugar común ni acceso a personas distintas de la usuaria.

2. *Archivo de registro de accesos: actividad, monitorización y seguimiento:*

    a) El uso de archivos de registro de accesos es una medida de seguridad importante que permite la identificación y el seguimiento de las acciones con los datos personales.

3. *Seguridad de los puestos de trabajo, servidores y redes:*

    a) Actualización: tienes que asegúrate de mantener la actualización de ordenadores y dispositivos en la media posible.

    b) Antivirus: en los ordenadores y dispositivos donde realices el tratamiento automatizado de los datos personales dispón de un sistema de antivirus, actualizándolo de forma periódica.

    c) Cifrado: la seguridad de la red es importante tanto respecto a las conexiones externas (por ejemplo, a Internet), como a la interconexión con otros sistemas (externos o internos) de la propia universidad. Cuando realices el acceso a través de Internet, cifra la información con protocolos criptográficos (TLS/SSL).

    d) Cortafuegos y detección de intrusos: monitoriza el tráfico hacia y desde el sistema de información con Cortafuegos y Sistemas de Detección de Intrusos.

    e) Segregación: la red de datos debe segregarse de las otras redes.

4. *Cifrado de datos:*

    a) Cuando precises mover datos personales, ya sea por medios físicos o por medios electrónicos, utiliza un método solvente de cifrado.

5. *Copias de seguridad:*

    a) Periódicamente realiza una copia de seguridad en un segundo soporte distinto del que utilizas para el trabajo diario. Almacena la copia en un lugar seguro, distinto de aquél en tengas ubicado el ordenador con los ficheros originales, así podrás recuperar los datos personales en caso de pérdida de la información.

6. *Destrucción adecuada de dispositivos y eliminación de datos.*

7. *Seguridad física de las instalaciones.*

Es evidente que todos los grupos de investigación van a tener que formarse y entrenarse en esta parte de las tareas para llevar adelante sus proyectos. Es importante que se plantee todo esto dentro del propio diseño de la investigación ya que requiere tiempo, trabajo y recursos humanos y materiales. Pero afortunadamente, siempre cuentas con un DPD en tu centro que puede ayudarte porque es su área de conocimiento y su competencia el hacerlo.

7 MEDIDAS TÉCNICAS DE SEGURIDAD DURANTE LA INVESTIGACIÓN

1. Control de acceso y autentificación: perfiles y contraseñas.
2. Archivo de registro de accesos: actividad, monitorización y seguimiento.
3. Seguridad de los puestos de trabajo, servidores y redes:
   - Actualización.
   - Antivirus.
   - Cifrado.
   - Cortafuegos y detección de intrusos.
   - Segregación de la red de datos de las otras redes.
4. Cifrado de datos.
5. Copias de seguridad.
6. Destrucción adecuada de dispositivos y eliminación de datos.
7. Seguridad física de las instalaciones.

7. Documenta con diligencia

Para finalizar en una labor de constatación y control, de este aspecto concreto de tu investigación, es necesario que tengas a punto y guardados una serie de documentos como los consentimientos firmados, el posible ejercicio de derechos de los interesados, la gestión de los incidentes, los compromisos firmados de confidencialidad y, en caso necesario, los contratos de encargados de tratamiento. Hay documentos que se generaran en el proceso de registro de tratamiento o gestiones con tu DPD que no es necesario que guardes personalmente. En los siguientes apartados figuran los documentos, cómo se generan y quién y dónde deben custodiarse.

Como responsable del proyecto de investigación tienes que poder demostrar que has actuado con diligencia en el cumplimiento de tus responsabilidades en la protección de datos personales. La mejor manera de hacerlo es documentando las tareas que realicéis en torno a dichos datos.

1. Registro de las actividades de tratamiento (RAT).
2. Custodia de consentimientos.
3. Registro del ejercicio de derechos.
4. Informe de análisis de riesgos.
5. Informe de evaluación de impacto (EIDP).
6. Registro de gestión de incidentes.
7. Compromisos de confidencialidad.
8. Contratos encargados de tratamiento.
9. Nombramiento de responsable de seguridad del proyecto de investigación.

No necesitarás todos estos documentos en todas las investigaciones, pero son todos los posibles según la legislación.

Documento 1. **Registro de las Actividades de Tratamiento (RAT)**

El Registro de las Actividades de Tratamiento es un documento obligatorio donde se recoge la lista de los tratamientos de datos que lleva a cabo la institución, entre ellos los correspondientes a proyectos de investigación. En nuestro caso, el RAT está en formato electrónico y puede consultarse en la página web de la UPV/EHU www.ehu.eus/babestu

Una vez solicites al DPD el registro del tratamiento de datos asociado a tu investigación, será incluido en el RAT (de la UPV/EHU o de la institución correspondiente). No es necesario, aunque sí conveniente, que lleves una relación de los tratamientos que tengas en el RAT.

La información que contendrá el RAT de tu tratamiento es la correspondiente a la segunda capa de información.

Documento 2. **Custodia de consentimientos**

Como persona IP responsable debes tener guardados, en formato electrónico o en papel, todos los consentimientos de los donantes, para el tratamiento de sus datos. Estos documentos te van a permitir, en caso necesario, demostrar la legitimidad para realizar dicho tratamiento. Tanto en formato papel o electrónico, debes guardarlos de manera segura en una ubicación que deberás detallar en el formulario de declaración del tratamiento. Tu DPD te asesorará sobre cómo hacerlo también.

Documento 3. **Registro del ejercicio de derechos**

Las personas participantes en tu investigación pueden ejercer sus derechos ARSOPL a través del DPD (de la UPV/EHU, en nuestro caso). Cuando ellas se dirijan al IP o a cualquier miembro el equipo investigador debe comunicárselo inmediatamente al DPD que llevará un registro de todas las solicitudes de derechos recibidas y las respuestas que se les han dado. Este registro se ubicará en la misma dirección electrónica que te ha facilitado el DPD en el momento del registro del tratamiento.

Documento 4. **Informe de análisis de riesgos**

El informe de análisis de riesgos ha de mantenerse actualizado y debe documentar el *análisis de riesgos* realizado, sus conclusiones y las *medidas de seguridad* adoptadas. Este documento también se incorpora de manera previa al registro del tratamiento en el RAT y se ubica en la plataforma o archivo que te ha asignado el DPD.

Documento 5. **Informe de Evaluación de Impacto (EIPD)**

Como ya sabes, en los proyectos de investigación con alto riesgo o con tratamiento masivo de datos especialmente protegidos, es obligatorio este informe o informes (si hay que volver a realizarlo por modificaciones en el proyecto de investigación).

Este documento está incluido en el formulario de declaración del tratamiento y se incorpora de manera previa al registro del tratamiento en el RAT que te ha asignado el DPD.

Documento 6. **Registro de gestión de incidentes**

Ya se ha mencionado que cuando se produzca una situación que afecte a los datos personales debes ponerte en contacto con tu DPD que debe registrar el incidente de seguridad y, en su caso, notificarlo a la Agencia Española de Protección de Datos.

Es conveniente llevar un registro de esos incidentes con una descripción de cada uno de ellos, los datos y las personas afectadas, las consecuencias y las medidas adoptadas. Este registro se ubica en la misma dirección electrónica o plataforma que te ha asignado el DPD en el momento que registraste el tratamiento de datos al diseñar tu investigación.

Documento 7. **Compromisos de confidencialidad**

Tendrás guardados, en formato electrónico (requiere firma electrónica) o en papel, todos los compromisos de confidencialidad firmados por las personas que acceden a los datos personales de tu investigación. Estos documentos también quedan ubicados en la misma dirección electrónica o plataforma que te facilitó el Delegado de Protección de Datos en el momento del registro del tratamiento.

Documento 8. **Contratos encargados de tratamiento**

Los contratos de encargado de tratamiento, si los hubiera, debes tenerlos firmados y guardados en formato electrónico (requiere firma electrónica) o en papel. En nuestra institución, por ejemplo, se dispone de un modelo oficial de contrato en www.ehu.eus/babestu *(«Compromisos a asumir por empresas externas que realizan tratamientos de datos por cuenta de la UPV/EHU», aprobado por el Consejo de Gobierno en sesión de 10 de abril de 2008*). Como el resto de la documentación, tienen que quedar recogidos en la plataforma o dirección electrónica facilitada por tu DPD.

Documento 9. **Nombramiento de responsable de seguridad del proyecto de investigación**

Como ya se ha expuesto, es recomendable nombrar a un miembro del equipo como responsable de seguridad y dejarlo reflejado en un documento en el que se indique quién es y cómo ha aceptado y entiende sus responsabilidades). Como el resto de la documentación, este nombramiento tiene que quedar recogido en la plataforma o dirección electrónica facilitada por tu DPD.

8. Anexo

Consentimiento informado para solicitar la participación en investigación y la utilización de sus muestras o datos

Para poner en marcha una investigación con seres humanos, ellos mismos o con sus muestras o con sus datos, es obligatorio que conste la manifestación de la voluntad libre y consciente para participar, válidamente emitida por personas capaces, o por sus representantes autorizados, precedida de la información adecuada (LIB art. 3f)).

Para llegar a esa manifestación, cada sujeto participante tiene que ser informado adecuadamente sobre la investigación y solo así podrá decidir. En el caso de estar pidiéndole sus datos se debe incluir información específica sobre ello y, además de la recogida del consentimiento para ser participante en una investigación, un apartado específico recogida del consentimiento para el uso de sus datos, tal como exige la normativa vigente.

ESTRUCTURA BÁSICA DE UN DOCUMENTO DE CONSENTIMIENTO INFORMADO

LOGO INSTITUCIONAL (UPV/EHU en nuestro caso)

IDENTIFICACIÓN DEL INVESTIGADOR RESPONSABLE

- Nombre y apellidos.
- Departamento y Centro.
- Datos de contacto: dirección email y teléfono institucionales.

DESCRIPCIÓN DE LA INVESTIGACIÓN (información obligatoria mínima)

- Identificación del proyecto: título y financiación.
- Breve resumen del proyecto:
  - — Objetivos y beneficios esperados.
  - — Duración.
  - — Lugar de realización.

DESCRIPCIÓN DE LAS INTERVENCIONES que se realizarán al sujeto reclutado:

- Tipo y descripción de prueba o intervención (encuesta, toma de muestra, grabación en audio, vídeo) y su objetivo.
- Número de veces que se va a realizar, fechas y plazos.
- Si va a haber contacto posterior con el participante.
- Descripción de riesgos y/o molestias y medidas para minimizarlos (incluido el seguro si procede).
- Ofrecimiento para aclarar las dudas, proporcionar más información y la forma de contacto para ello.

VOLUNTARIEDAD

Decide si quiere o no participar. Se le informa de que su participación es voluntaria y que la negativa a hacerlo no supondrá ningún perjuicio o medida en su contra.

REVOCACIÓN

Se le informa de que puede retirarse de la investigación cuando quiera sin consecuencias personales en cualquier momento y sin necesidad de dar explicaciones. Se le informa también, de con quién contactar (IP) y dirección de contacto institucional para hacer efectiva la revocación.

DESTINO DE SUS MUESTRAS

Se le informa para que decida qué puede hacerse con sus muestras tras finalizar la investigación:

- Destrucción.
- Anonimización.
- Cesión gratuita a Biobanco, identificándolo.
- Conservación en colección de muestras para investigaciones relacionadas con la inicialmente propuesta.
- Otro destino.

PROTECCIÓN DE SUS DATOS

Cuando aporte datos personales se le informa de que, de conformidad al Reglamento Europeo de Protección de Datos (UE2016/679),

Los datos personales que se le solicitan son . . . . . .
El código del tratamiento de datos es . . . . . .
El nombre del tratamiento de datos es . . . . . .
La finalidad de este tratamiento es . . . . . .
El responsable del tratamiento de datos es . . . . . .

En nuestro caso constará la UPV/EHU: Identidad Universidad del País Vasco/Euskal Herriko Unibertsitatea CIF: Q4818001B Dirección postal: Barrio Sarriena s/n, 48940-Leioa (Bizkaia) Página web: www.ehu.eus Datos de contacto del Delegado de Protección de Datos: dpd@ehu.eus)

El periodo de conservación de sus datos será . . . . . .

La legitimación del tratamiento es su consentimiento informado.

Las posibles cesiones y transferencias internacionales de sus datos indicando si se cederán y a quién o si no se cederán.

Cesiones

NO: «A esta información no podrá acceder ninguna persona externa al proyecto, salvo en cumplimiento de una obligación legal».

SÍ: «La información que usted nos facilite será accesible por otros investigadores o universidades, precisando a quién y por qué».

Transferencias internacionales

NO: «Los datos no serán transferidos a otros países ajenos a la Unión Europea».

SÍ: «Los datos serán transferidos a otros países ajenos a la Unión Europea».

Los derechos sobre sus datos que son los de acceso, supresión, rectificación, oposición, limitación del tratamiento, portabilidad y olvido.

En nuestro caso puede ejercerlos enviando su petición a dpd@ehu.eus. Tiene a su disposición información adicional en http://www.ehu.eus/babestu La información completa sobre este tratamiento está en: https://www.ehu.eus/es/web/idazkaritza-nagusia/ikerketa-datu-pertsonalen-tratamenduak

Destino de los datos: se le informa de qué se hará con sus datos cedidos para la investigación, una vez que ésta finalice:

- Destrucción.
- Anonimización.
- Cesión, identificando a quién.
- Conservación para investigaciones relacionadas con la inicialmente propuesta.
- Otro destino.

GRATUIDAD

Se le informa de que la participación donando sus datos, sus muestras, respondiendo encuestas, etc., es altruista y por lo tanto no habrá remuneración por ella. Si hubiera una compensación se describirá.

ACCESO A RESULTADOS DE LA INVESTIGACIÓN

Se le informa de que puede conocer los resultados de la investigación, poniéndose en contacto con la persona responsable de la investigación.

En el caso de *datos genéticos*, se le informa de las posibilidades:

- Posibles descubrimientos inesperados.
- Derecho a no saber.
- Información a familiares.
- Consejo genético.

FIRMAS DE CONSENTIMIENTO PARA PARTICIPAR EN LA INVESTIGACIÓN

- Identificación, fecha y firma de la persona encargada de informar y de recoger el Documento de Consentimiento.
- Identificación, fecha y firma de la persona que presta el consentimiento a participar en la investigación:
  - — Menor de 12 años: identificación y firma del representante legal.
  - — Mayor de 12 años y hasta 18 años: identificación y firma de consentimiento del representante legal e identificación y constancia de asentimiento del menor.

FIRMAS DE CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS

- Identificación y firma de la persona que consiente a la utilización de sus datos personales en las condiciones descritas en el punto PROTECCIÓN DE SUS DATOS de este documento:
  - — Para datos de menor de 12 años: firma del representante legal.
  - — Para datos de mayor de 12 y menor de 14 años: firma del representante legal y constancia de asentimiento del menor.
  - — Para datos de mayor de 14 años: firma del menor.
  - — Para datos de menor de 18 años en una investigación invasiva (riesgo psíquico durante la obtención): firma del representante legal y constancia de asentimiento del menor.

A Guide to Data Protection in Human Research

Based on the new European Regulation on Data Protection (GDPR) and Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPD-GDD)

Index

Introduction

The protection of personal data is based on the desire to defend people's freedoms and privacy. It is an ethically valuable task that has been translated into concrete laws. This must always be kept in mind in order to act responsibly, and not merely to comply with the law. When this conviction is assumed, it is easier to resolve the doubts and specific situations regarding data protection, and consequently to take adequate care of people's privacy and autonomy.

USE OF PERSONAL DATA IN RESEARCH: It is the responsibility of researchers to protect those who have agreed to be part of the scientific investigation, whether the research requires the use of personal data, human biological samples or direct involvement of volunteers.

This brief manual is intended to help you provide the proper care for participants, or donors, of the data that will be used in research activities; whether it be basic, applied or supervised research such as doctoral theses, master's theses or final papers. This care we owe to the data subjects is specified in the protection of their privacy and freedom, promotion of confidentiality and compliance with current legislation.

These are the questions you should take into account when designing a project before starting your research activity, if you will require personal data.

20 Basic Questions FOR Organizing Your Research Project

1. What is the title of your research activity?
2. Do you need people to provide you with information about themselves for you to perform the research?
3. What kind of specific information do you need?
4. For what purpose, from a methodological point of view, do you need these data?
5. Will you obtain these data directly from people?
6. Through what instruments (survey, interview, medical history) will you extract and collect the data?
7. Have you prepared a document with specific, sufficient and truthful information to explain what you are going to ask data subjects and what you are going to use this information for?
8. Have you included in the document information on what their rights are and how they can exercise them?
9. If you obtain the information from sources other than data subject, how will you do it?
10. When you have the data, will you pseudonymise it by separating the data and identities with codes to avoid personal identification?
11. Where will you store the data and work with it for the length of your research?
12. Who will be able to access and use the data to carry out the research activity?
13. How long will you need to work with the data and retain it afterwards?
14. Do you plan to give the data to people outside your research team?
15. What harm could it do to the data subjects if data were lost or used illegally?
16. What damage would it do to the research if you were unable to access the data collected?
17. What mechanisms do you have to ensure that the data will not be used illegally, lost and that access is not blocked?
18. Have you established any protocol, document or tutorial to transmit to your research team the safety needs and obligations generated by the use of personal data?
19. Have you have prepared any document to record everything you are doing to protect the information collected for your research?
20. Have you contacted your institution's data protection officer (DPO) to help you think through and develop an appropriate data protection policy?

The answers to these questions, from the requirements of the regulations, can be summarized in seven steps:

1. **Identifying 10 basic aspects:** (1) If personal data are involved, (2) the purpose for which it will be used, (3) data origin, (4) the data subjects (recruits/donors), (5) If it is sensitive data, (6) the processing that will be carried out on these data, (7) the persons responsible for the processing, (8) possible transfers to third parties, (9) possible international transfers, (10) contact the data protection officer (DPO).
2. **Acting lawfully:** By complying with the conditions for lawful[1] processing of personal data in research, particularly if it is sensitive data. In research activities, the legitimacy of the processing is typically based on the informed consent of the data donors, although exceptionally there may be other bases of legitimacy.
3. **Informing:** provides data subjects, who give you their data, all necessary information, including the possibility of exercising their rights[2].
4. **Obtaining explicit consent**[3] of data subjects.
5. **Carrying out a risk analysis:** Assumes responsibility for the care of the persons from whom you obtain the data. Contact your centre's DPO to carry out an analysis of the risks of processing personal data, and if necessary, an impact assessment.
6. **Ensuring safety:** Applies technical security measures and appropriate organizational measures, taking into account the identified risks.

---

[1] The collection, storage, use, preservation and even transfer of data.

[2] AREOPL (access, rectification, erasure, objection, portability and limitation) rights.

[3] **Explicit:** The data subject issues an express declaration of consent (clear affirmative action), e.g. signing a document or clicking on the action 'I accept' in an electronic environment.

7. **Documenting diligently,** with the help of your centre's DPO, how your processing is noted in the Records of Processing Activities at the UPV/EHU or at the centre where you are researching in order to: (1) specify how to store the signed consent forms, (2) document the data subjects' exercise of rights in coordination with the subjects, (3) carry out the risk analysis, and where appropriate, (4) the impact assessment, (5) manage incidents, (6) collect confidentiality commitments, and where necessary, (7) the contracts of processors.

The Seven Steps of Data Protection in Human Research

STEP 1. Identifying 10 basic aspects:

1. If personal data are involved.
2. The purpose for which they will be used.
3. Data origin and how you will collect it.
4. The data subjects/recruits/donors.
5. If there are sensitive data.
6. The processing that will be carried out: filing, organizing, analysing, storing, etc.
7. The party responsible for the processing during this stage of the project: Institution or research centre, principal investigator (PI) or delegated person.
8. Possible transfers to third parties.
9. Possible international transfers.
10. CONTACT YOUR DATA PROTECTION OFFICER.

STEP 2. Acting lawfully. Makes the processing lawful.

STEP 3. Informing. Provides the data subjects with all necessary information, including the possibility of exercising their rights.

STEP 4. Obtaining explicit consent of the data subjects.

STEP 5. Carrying out a risk analysis. Assumes responsibility for the care of the persons from whom you obtain the data. Contact your centre's DPO to carry out an analysis of the risks of processing personal data, and if necessary, an impact assessment.

STEP 6. Ensuring safety. Applies technical security measures and appropriate organizational measures, taking into account the identified risks.

STEP 7. Documenting, with the help of your DPO, to:

1. Record your processing in the registration of the research centre's processing activities.
2. Specify how the data should be stored.
3. Readying the mechanism for the exercise of ARDOPL (access, rectification, deletion, objection, portability and limitation) rights.
4. Conduct a good risk assessment, and where appropriate, an impact assessment.
5. Provide for the management of possible incidents.
6. Collect signed confidentiality commitments.
7. Record the contracts of processors (if any).

1. Identifying

Think and project: (1) If personal data are involved, (2) the purpose for which it will be used, (3) data origin, (4) the data subjects (recruits/donors), (5) If it is sensitive data, (6) the processing that will be carried out on these data, (7) the persons responsible for the processing, (8) possible transfers to third parties, (9) possible international transfers, (10) contact your centre's DPO.

Personal Data

'Personal data' refers to any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data: Any numerical, alphabetical, graphic, photographic, acoustic or other information of identified or identifiable natural persons.

Purposes and Source

You must be very clear when designing future research as to why and for what purpose you are obtaining, recording, studying and storing the data, etc., and also that you cannot process them later in a manner that is incompatible with these purposes, as personal data must always be processed for specific, explicit and legitimate purposes.

You should also take into account the criterion or *principle of data minimization*: you should only collect the data that are essential for carrying out the research, but do not collect data that are not included in the initial design of the project or 'just in case they are needed later'.

Logically, you also need to foresee and record in your project where you will obtain this information (directly from the data subject, medical records, historical documents or other indirect sources).

THE 5 Ws OF PURPOSES AND SOURCES

WHAT: Accurately describe the information or type of data you need to collect.

Data minimization principle: Only essential data are collected.

WHY: Clearly state for what purposes you are collecting, recording, studying, analysing, processing, storing the data, etc.

Purpose limitations: You cannot process data further in a manner that is incompatible with those purposes.

WHERE: Specify where you will collect the data; whether directly from the data subject, medical records, reports, files or other indirect sources and whether it will be via interviews, surveys, tests, cards, etc.

Confidentiality.

WHO: Determines the profile of the volunteer data subjects and who will do each processing.

Informed consent.

WHEN: Arrange the times of each step: collection, pseudonymisation, preservation, transfer, etc.

Categories of Data Subject

The legislation terms 'data subject' those who grant you personal information that you will transform into data for your research activity.

In fact, they are the people recruited or donors for the research activity. Those to whom, once you have explained why you need them, for what purposes and in what way you will use and protect their data, grant you the information requested.

Special Categories of Data

There are data that you may need for research, and because of their relevance to people's privacy, you have to process them with greater care and meet a number of requirements.

Not all personal data are the same and the regulations classify them as follows:

Special Categories of Personal Data, or Sensitive Data

Personal data that are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection, as the context of their processing could create significant risks to fundamental rights and freedoms (GDPR Article 9; Recital 51-56).

This includes data revealing:

- Political opinions.
- Union membership.
- Religious or philosophical beliefs.
- Racial or ethnic origin.
- Data concerning health[1].
- Data concerning a natural person's sex life or sexual orientation.
- Gender violence and abuse.

- Genetic data[2].
- Biometric data[3].
- Data on convictions and criminal offences.
- Data relating to administrative sanctions.

All kinds of sensitive data are frequently used in university and other research activities, as research is carried out in the biological, biomedical, technical, social, legal and behavioural sciences. They are particularly sensitive:

[1] **Data Concerning Health:** All data pertaining to the data subject's health status that reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or another health professional, a hospital, a medical device or an in vitro diagnostic test.

Always bear in mind that, for the collection, use, conservation, etc., of this information, the data protection regulations are complemented, among many others, by the Ley de Autonomía del Paciente (Law on Patient Autonomy 41/2002), which regulates the rights and obligations regarding clinical information and documentation and which includes communication, decision-making, informed consent, access to clinical records, etc.

[2] **Genetic Data:** Specific health-related data relating to the inherited or acquired genetic characteristics of a natural person that result from the analysis of a biological sample from that natural person, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained (GDPR recital 34).

[3] **Biometric Data:** Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person that allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (GDPR Article 4.14).

Children's Data

In principle, these are not sensitive data, but the regulations state that, due to their condition of vulnerability, you must treat them as such, as these people may be less aware of the risks, consequences, guarantees and rights concerning the collection and use of their data, and it is your responsibility to prevent them from being violated.

As a guideline, consider that if the data you intend to request could generate serious tension or affect the child, it would be considered an invasive investigation and you will have to seek consent from the legal representatives (parents or guardians), and ensure that the child, aged 12 years and above, agrees. When the data are not of that type, you will only require the legal representatives' authorisation for minors aged 14 years; from this age, they are the ones who can grant authorisation. The DPO and the ethics committee that will evaluate your project can advise you on the doubts that may arise, as the casuistry varies greatly and the law is not restrictive on this matter.

Type of research	Age	Consent
Invasive research with data	Under 18 years	Legal representatives' consent. Agreement from the 12-year-old.
Non-invasive research with data	Under 14 years	Legal representatives' consent. Agreement from the 12-year-old.

Personal Data of Vulnerable Data Subjects

Special care must be taken if the research activity involves the use of data on people from particularly vulnerable groups, such as children (mentioned above), the disabled, the elderly, people at risk of social exclusion, people in compromising political situations, the undocumented, etc.

SPECIAL CATEGORIES OF PERSONAL DATA, OR SENSITIVE DATA

Political opinions
Union membership
Religious or philosophical beliefs
Racial or ethnic origin
Data concerning health
Data concerning a natural person's sex life or sexual orientation
Gender violence and abuse
Genetic data
Biometric data
Data on convictions and criminal offences
Data relating to administrative sanctions

It is quite common to use data with a particular impact on the privacy, public freedoms and fundamental rights of the subject, as research is carried out in the biological, biomedical, technical, social, legal and behavioural sciences.

Data Processing

Data processing refers to any operation or set of operations performed on personal data, personal information transformed into data or a set of personal data, or data that, not being personal, its aggregation identifies a person, whether by automated procedures or not. Thus, collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction are data processing.

A research activity may involve one or more processing of personal data. In fact, you will always have to 'process' information about the members of your own research team (personal data) and sometimes about people whose data you need to carry out the research.

DATA PROCESSING

Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as:

- Collection.
- Recording.
- Organisation.
- Structuring.
- Storage.
- Adaptation.
- Alteration.
- Pseudonymisation.
- Anonymisation.
- Retrieval.
- Consultation.
- Use.
- Disclosure by transmission.
- Dissemination.
- Enabling access.
- Comparison.
- Alignment or combination.
- Limitation.
- Deletion.
- Destruction.
- Etc.

Examples of data processing are the management of information (collection, archiving, use) on the researchers, and although this is not data processing for research, the management of information requested from participants (collection, archiving, use), pseudonymisation, coding or dissociation, preserving written documents of informed consent, etc.

This term can lead to confusion, because the processing of data in a research activity usually refers to the statistical or analytical method used for drawing conclusions from the data obtained in the experiments, carried out in the laboratory, in the samples, in field work or in any other area in which the methodology specific to each scientific activity is being applied.

Data Controller

This is the natural or legal person who is responsible for the processing of the data and who must always be identified as such in any research.

For example, the UPV/EHU is responsible for all research processing registered in its record of processing activities (ROPA). In fact, the main researcher, tutor or thesis director, TFMs or TFGs[4], is considered the internal data controller for practical purposes, but it is always the UPV/EHU that is responsible for all processing with personal data that takes place at the university institution.

When, as a researcher, you need the services of a person or a company that processes personal data on your instructions, such as an IT service company, it is compulsory for the institution, in our case the UPV/EHU, to sign a data processing agreement with that natural or legal person.

[4] TFM, in Spanish, Trabajo de Fin de Máster; TGF, Trabajo de Fin de Grado, it refers to final máster and degree reports.

Data Transmission Or Data Communication

If you have to provide personal data to third parties outside the research (third parties are those who are NOT the data subject, controller, processor and persons who are under the direct authority of the controller or processor), it is mandatory that you obtain the subject's express and written consent.

There is a special situation you should consider: if the information you are going to communicate to third parties includes data obtained from the data subject, which reveals or may reveal *personal information about their relatives*, this transmission will also require their express written consent.

International Data Transfers

This refers to the transfer of personal data to countries outside the European Union (EU), or international organisations. Both you as a researcher and the institution where you are performing your research, which is responsible for the processing, will be exporters, as you are in European territory and you are going to carry out this international transfer.

You can only make transfers of the personal data of research to a country or international organization if they guarantee an adequate level of protection in accordance with the conditions established in Chapter V of the GDPR. When the data are to be transferred outside the EU to any country, territory or specific sector of that third country or international organization that the European Commission has not considered to guarantee an adequate level of protection, some of the circumstances collected in the aforementioned chapter must occur to authorize said transfer. The casuistic extension of GDPR conditions exceeds the claims of this guide. Consult chapter V, or better consult, with your centre's DPO.

If personal data from the research are to be hosted in the 'cloud' (cloud computing), it is important to be aware that many of the companies providing such services are located outside the EU and do not provide adequate legal safeguards. In this case, please remember that it is essential that you consult your DPO, who will be able to gather this information.

Data Protection Officer (DPO)

> The person acting as Data Protection Officer must be a solver of all situations related to the processing of personal data that may arise. They are neither controller nor in charge of the data processing, because assuming such tasks would compromise neutrality, but are a figure who has a central role in organisations where special categories of personal data are processed. (Sánchez Ors, 2019)[5]

The DPO is a data protection specialist that public and private universities and other institutions are obliged to appoint. This DPO is responsible for informing, advising, assisting and responding to all queries on data protection from the entity responsible (in our case, the UPV/EHU) and also from the internal data controller (in our case the principal investigator (PI) or the person designated by the research team).

The DPO has to ensure that legal obligations regarding data protection are met, also by ensuring and cooperating with the controlling authorities (the Spanish and Basque data protection agencies AEPD and AVPD, respectively).

As a researcher, you must contact this person for everything related to the processing of personal data in your research, as among their functions are:

1. Informing and advising you.
2. Assisting you and supervising risk analyses, impact assessments and compliance with their application in the various research projects.
3. Controlling, coordinating and verifying the security measures applicable in the case of your investigation.

The DPO is also always a member of the research ethics committee (REC) that will report on your project, so the relationship between your research tasks with personal data and your work as a DPO are mandatory, direct and constant.

---

[5] Translated from Spanish.

DATA PROTECTION OFFICER

The relationship between your research tasks with personal data and your work as a DPO are mandatory, direct and constant.

- Informs, trains and advises.
- Assists and monitors risk and impact assessments and compliance.
- Controls, coordinates and verifies the applicable safety measures.
- Supervises incidents management.
- It is a reference for data subjects on data protection and the exercise of rights.
- Supervises the organisation of the institution's data protection information and documentation.
- Is a member of the REC that reports on the methodological, ethical and legal aspects of research projects.
- Is the link to the regional and national data protection authorities.

2. Acting Lawfully

This simply means that you comply with the conditions for the lawful processing of personal data in your research.

Lawfulness of Processing

Also termed 'legal basis', which allows you to use data in your research activity: once you have identified the data you are going to collect, from whom, and the processing you are going carry out, it will only be legitimate for you to do so if you have the informed consent of the data subject, who must give their consent by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of their agreement to the processing of personal data relating to them, such as by a written statement, including by electronic means, or an oral statement (GDPR Article 6(1)(a); Recital 32).

Other legal bases for the processing of data include legal obligation, vital interest, public interest and legitimate interests. In research involving human beings, do not detract from or replace your duty of information and consent, only reflect some situations in which the data subject knows that there is a public interest (LOPD Article 8 and GDPR Article 9).

General Conditions Governing the Lawfulness of Processing Sensitive Data

Although the collection, use or storage, i.e. processing, of sensitive data is generally prohibited, you may process sensitive data for your research if you meet one or more of the following conditions:

- You have the subject's explicit consent for a specific research activity purpose.
- These data are necessary for archiving and public interest purposes, scientific or historical research purposes or statistical purposes and are pseudonymised by others.
- There are public interest reasons in the field of public health.

Moreover, you are required to meet the following requirements:

a) Obtain explicit written consent from the recruits confirming that they agree to grant you their data, the specific purpose of processing and how it will be processed.

b) Ensure the quality of the data, i.e. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

c) Also ensure that the data are not collected in an unlawful, fraudulent or illicit manner.

d) In case you collect data concerning health, you must provide any information you obtain related to the data subject's health that is useful to the subject.

e) Assess the necessity and proportionality of the processing operations in relation to the purposes.

f) When you need health data from the data subject's clinical record, always collect a sheet or document of information and consent that includes:

   - The name of the professional and the centre where the patient has been treated.

- The purposes of the petition.
- Expression of conformity of publication of the clinical case in scientific publications addressed to health professionals.
- The patient's name.
- The patient's identity card or passport and signature expressly authorizing the use of their clinical record data under the conditions described in the report.

g) Ensure compliance with the statutory obligation of confidentiality by the people who have access to the data, even when the relationship between the parties has ended.

> Spanish Criminal Code, Article 199: 1. Anyone who reveals another person's secrets, which he or she knows because of his or her trade or employment relations, shall be punished by imprisonment of one to three years and a fine of six to twelve months.
>
> 2. A professional who, in breach of his obligation of secrecy or confidentiality, discloses the secrets of another person shall be punished by imprisonment for one to four years, a fine of 12 to 24 months and special disqualification from that profession for a period of two to six years.

In this case, as in others, the greatly varying casuistry provided by research and the imprecision of the law, which was not written with research alone in mind, make it essential to seek the guidance of your centre's DPO and REC, who will know how to consider these questions prudently and practically.

Special Circumstances for Lawful Use of Data Concerning Health in Scientific Research

In health-related research, especially in biomedicine, there are two special circumstances in which you may lawfully use personal data:

1. The reuse of personal data for health and biomedical research purposes shall be considered lawful and compatible when, having obtained consent for a specific purpose, the data are used for research purposes or areas related to the area in which the initial study was scientifically integrated. For example, the consent was given for the processing of research data on a certain type of cancer and you want to continue processing it for general oncology research. In this case, you have to inform those affected and you need a prior favourable report from the REC.
2. The use of pseudonymized personal data for health research purposes, and in particular, biomedical research, is considered lawful. The DPO will help you ensure that you are committed to confidentiality and that re-identification will not occur.

(See the 17th additional provision of the LOPD-GDD.)

3. Informing

Provide those who are will provide data for your research with all the necessary information, including the possibility of exercising their rights, in clear and simple language, in a concise, transparent, intelligible and easily accessible manner.

Who has to Inform and When?

The duty to inform data subjects about the aspects referring to the processing of their data corresponds to the person internally responsible for the research activity (PI or the person designated by the PI), who has to inform on behalf of the institution, i.e. the UPV/EHU in our case.

Logically, you must always make all the information available to candidate subjects before collecting the data.

Exceptions to the Duties of Providing Information

You do not have to report when:

- The data subject already has the information.
- It is impossible or disproportionate to inform, in such case you will have to take appropriate and concrete measures to protect their rights.

How to Inform?

To inform correctly, you must adapt the information to the data collection model you will use and to its characteristics, which will vary in extension, space, clarity, possibility of relating information, etc:

- Oral: Face to face or when you speak to someone on the telephone.
- In writing: Printed media, printed adverts, forms such as financial applications or job application forms.
- Electronic: Text messages, websites, emails, mobile applications.

Remember that diligent compliance with data protection requires you to keep a record of what you have reported, and it is therefore advisable to provide the first-level or first-layer information in writing in the Consent Document, so that you can sign for its receipt, and always with the link to access the complete or second-layer information. The following section explains what comprises the two-layer information.

Reflect, imagine and organize with an integral vision the information and the collection of the consent that you require for your research activity, so that the person concerned is not overwhelmed or confused.

The characteristics of good information are always simplicity, clarity, conciseness, transparency, intelligibility and easy access.

Presentation of the Information by Layers or Levels

The LOPD-GDD introduces this concept of information by layers or levels, referring to how to present the information to the person from whom you request the data.

In the first level you inform them:

- in a concise way
- at the very same time
- in the same medium in which you will collect the data.

You can then provide further information on a second level:

- with a more detailed presentation of the information
- using the medium you consider most appropriate for its presentation, understanding, and if you wish, for its archiving.

Example: A paper document requesting informed consent (IC) to participate in research, which includes IC for the donation of data needed for research, contains the first layer of information, and the same paper document includes a link to the website where the second layer of information is located (IC Document Annex).

First Layer or Level Of Information

The basic content of the information you provide to the donor corresponds to the so-called 'first layer' or 'first level of information' in the standard and is what potential donors need to know in order to decide whether or not to agree to give you their data:

1. Processing code (code in the ROPA).
2. Label of the processing.
3. Controller (Institution: UPV/EHU in our case).
4. Data source when it does not come from the data subject.
5. Purpose of data processing.
6. Lawfulness of data processing.
7. Recipients of international data transfers and communication.
8. Rights (access, rectification, erasure, objection, portability and limitation (AREOPL)).

This information will be provided to you by the Data Protection Office when you register your processing in the ROPA.

Second Layer or Level Of Information

In the second level of detail, you will include the following information:

1. Processing code (code on the ROPA).
2. Title of the treatment.
3. Data controller: Contact details of the UPV/EHU and the DPO.
4. Source of the data when it does not come from the data subject (extended).
5. Purpose of data processing.
6. Data retention period.
7. Lawfulness of data processing.
8. Recipients of international data transfers and assignments.
9. Personal data (exhaustive list of the data to be processed in the research).
10. AREOPL rights and how to exercise them.
11. Additional information (link to the UPV/EHU personal data protection website).

This information will be provided to you by the DPO when they register your processing in the ROPA.

INFORMATION FOR DATA SUBJECTS

Content

- Truthful and sufficiently extensive, precise, clear and intelligible.
- It is advisable to provide all first-level or -layer information in writing in the Consent Document.
- Always provide the access link to the complete or second-layer information.

Form

- Adapts the information to the data collection model:
  - Oral: Face to face or when you speak to someone on the telephone.
  - In writing: Printed media, printed adverts, forms such as financial applications or job application forms.
  - Electronic: Text messages, websites, emails, mobile applications.
- Include in the same Consent Document, if possible, information on the research in which you are asking the subject to participate and on the data you are requesting for it, and the two consent requests.

Custody

- Retain, in the most appropriate format, the proof that you have informed and that the subject has consented.

CEISH[6] UPV/EHU Recommendation on How to Inform

Submitting the basic information (first layer) and referring to the complete processing information in the public ROPA of the UPV/EHU (second layer) is a legal option. However, the CEISH UPV/EHU recommends including the following clause in the informed consent document—duly adapted to each research—under a heading that reads Data Protection Information:

- You are informed that in accordance with the European Data Protection Regulation (UE2016/679):
- Data processing code: . . . . . .
- Heading of data processing: . . . . . .
- The purpose of this processing is: . . . . . .
- Data controller UPV/EHU:

Identity: Universidad del País Vasco/Euskal Herriko Unibertsitatea

CIF: Q4818001B

Postal address: Barrio Sarriena, s/n, 48940 Leioa (Bizkaia)

Website: www.ehu.eus

Data Protection Officer: dpd@ehu.eus

- The personal data requested are: . . . . . .
- The retention period of your data will be: The data will be kept for as long as no request for erasure is made by the person concerned, and in any event, for as long as the time limits for appeals and/or complaints are open or for as long as they continue to serve the purpose for which they were obtained.

[6] Comité de Ética de Investigación con Seres Humanos/Human Research Ethics Committee.

- The lawfulness of the processing is: Your informed consent (or other sources of lawfulness if applicable).
- Transfers: (Indicate the transfers or if not noted, 'No data will be transferred except as provided by law').
- International transfers of your data: (Indicate the transfers or if not noted, 'No international transfers will be made').
- The rights on your data are those of access, erasure, rectification, opposition, limitation of processing, portability and erasure. You can exercise them by sending your request to dpd@ehu.eus
- Further information is available at http://www.ehu.eus/babestu
- Complete information on this processing is available at: https://www.ehu.eus/es/web/idazkaritza-nagusia/ikerketa-datu-pertsonalen-tratamenduak

If you feel that the data protection information presented in this manner is cumbersome or difficult to understand for the people participating in the research, you can attempt to adapt it to their profile, but keep in mind that it is mandatory to report all the points that appear in the basic information (first layer).

Information on Rights of Access, Rectification, Erasure, Opposition, Portability and Limitation (AREOPL)

This information on rights is always intended to promote decision-making and control over one's own personal data. Therefore, as the person responsible for the investigation, you have to inform the data subject about their rights, how they can exercise them and how to contact you in order to do so:

- Right of **A**ccess or right to request information from the data controller as to whether their data is being processed and if so what data it is.
- Right of **R**ectification or right to request amendment of data that is inaccurate or incomplete.

- Right of erasure or right to request the **Erasure** of data in certain cases, but the results already obtained shall not be deleted.
- Right to object or right to **O**ppose the processing of their personal data on grounds related to their particular situation.
- Right to Data **P**ortability or the right to request that data be provided in a structured, commonly used, machine-readable format and the right to have it transferred to another controller.
- The right to **L**imit the processing or the right to request that the processing of their data be limited under certain conditions.

PROMOTE SUBJECT'S DECISION-MAKING AND CONTROL OF THEIR PERSONAL DATA
AREOPL RIGHTS

RIGHT OF ACCESS: To know whether their data are being processed and if so, what data they are.

RIGHT OF RECTIFICATION: To request amendment of inaccurate or incomplete data.

RIGHT TO ERASURE: To request the erasure of data in certain cases.

The results already obtained shall not be deleted.

RIGHT TO OBJECT: To oppose the processing of personal data on grounds related to the data subject's particular situation.

RIGHT TO DATA PORTABILITY: To request data be provided in a structured, commonly used, machine-readable format and the right to have it transferred to another controller.

THE RIGHT TO LIMIT THE PROCESSING: To request that the processing of personal data be restricted under certain conditions.

As the person responsible for the research, the institution and the PI are obliged to inform the data subject about these rights, how they can exercise them and how to contact them in order to realise it.

Storage Period Information

When reporting the storage period on the IC, you must indicate to the potential data subject that the minimum storage period is 5 years for the purpose of auditing and verifying the research conducted with these data. You will also inform them that you can keep the data collected for the research as long as they do not request its erasure and that these data still serve the purpose for which they were obtained. The data subject cannot demand that you delete the results obtained with their data until the time of the erasure request.

Finally, please remember that if you apply the appropriate technical measures, such as anonymisation, you can keep the data longer.

DATA STORAGE PERIOD

- Minimum storage period is 5 YEARS for the purpose of auditing and verifying the research.
- May be kept longer for the purpose for which they were obtained if there is no request for *erasure*.
- The data subject cannot ask you to delete the results obtained with their data until the time of the erasure request.
- With appropriate technical measures, such as anonymisation, you can keep the data longer

This should be indicated on the information sheet and IC document.

Information on Possible Transfer of Data

To share, communicate and allow another person to access or transfer the data to a third party, the data subject must be aware of the possible transfer, as they would be the person who can permit such transfer.

The simplest approach is to include the request for transfer in the data protection information section, with a specific space for obtaining consent, in the IC document. If you do not intend to do so, specify that there will be no transfer in any case. International transfer takes place

when the data are to be transferred outside the EU territory or to countries that do not guarantee an adequate level of protection according to the European Commission.

* The communication of data to a processor (see point 1), with whom you have signed a contract is not considered a transfer of data, as the data processor will only process the data according to your instructions.

Further Processing or Additional Uses of the Data

It may happen that, once the subject has been informed and has accepted, you consider a new research with a new data processing compatible with the previous one. In this case, you will have to inform the subject by mail, electronically or other means, and you will need a *previous Favourable Report from the REC*.

4. Obtaining Explicit Consent

> 'Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.' (GDPR Article 4(11)

There is a specific provision in the new Spanish regulations (Additional Provision 17) on the processing of data concerning health—sensitive data—which states that, the data subject's consent is required for research with this kind of data, unless the data are pseudonymised. In this case, technical and functional separation is required between your research team and those who will perform the pseudonymisation and store the information that makes re-identification possible. In other words, it is not enough to guarantee that you or someone from your research team will perform the pseudonymisation when the donor's consent is not available.

The requirements for sensitive data in health research are also applicable to other areas of research—the biological, biomedical, social, legal and behavioural sciences—as far as sensitive data are concerned. The new regulation has not changed essentially, but is more demanding of express consent, as tacit consent was previously accepted, although it certainly referred mainly to situations of commercial transactions.

In summary, the new legislation reinforces the need for consent as a general rule, while offering, in the case of health research, the possibility of the use of pseudonymised data by third parties. In any case, this is an aspect that will help you prudently discern both the DPO and the REC of your centre.

Characteristics of Consent

The data subject's consent is the free expression that they accept that you treat their information, i.e. their data, for a specific purpose, under certain conditions of which they have been previously informed.

EXPLICIT

FREE

INFORMED

UNAMBIGUOUS

SPECIFIC

VERIFIABLE

DISTINCT

EXPRESS

REVOCABLE

Currently, there remain practices that were part of the so-called tacit consent. Nonetheless, they are no longer acceptable: silence, inaction or pre-selected boxes as a means of obtaining consent, as a supposed acceptance of the transfer of data, are no longer valid. It is only considered done in an appropriate manner when it is:

- *Explicit:* The donor subject issues an explicit declaration of consent (always a clear affirmative action), e.g. signing a document or clicking 'I accept' in an electronic environment.
- *Free*: Given in a context of freedom, it cannot be conditioned on, for example, a reduction in an academic task, the achievement of a material good, or any other type of condition. In assessing whether consent has been freely given, you should always take

into account the possible existence of conditions limiting such freedom of decision.

- *Informed*: For consent to be truly informed, the person concerned must know and understand upon what they are deciding, and to do so, it must be explained to them in a comprehensible manner as set out in Chapter 3.
- *Unambiguous*: The information is very clear and not mixed with other conditions of the research or with requests for donation of samples, conducting surveys, etc. (See Chapter 3, 'How to Inform').
- *Specific*: You must obtain consent for each purpose and explain thoroughly that you will not use the data for other purposes.
- *Verifiable*: As the person responsible for the data processing, you must be able to demonstrate to any competent authority, person or relevant committee that the data subject consented to the processing of their personal data for the purposes of your research.
- *Distinct and express*: If consent for the collection, use and retention of data is given by the person concerned in the text and in the context of consent to participate in your research project, you must present the information in a way that is clearly distinguishable from other matters in an intelligible and easily accessible form and using clear and simple language.
- *Revocable*: The data subject must be able to withdraw consent at any time, and you must inform them that they can request it simply without consequences and how they can do so.

Validity of the Consent Obtained before GDPR

If you obtained consent before the GDPR came into force—May 2018—you are not obliged to seek consent again under its conditions, as that rule did not apply when you were granted consent. For the sake of diligence and honesty, it is recommended that you provide the new information, as far as possible.

Consent Collected Electronically

The informed consent obtained in this manner is as valid as that on paper. If you do not want to have paper documentation and prefer to have everything in electronic format, you can even collect it with a digital signature or electronic certificate. Remember that, in all cases, the person concerned must take a clear affirmative action for their consent to be considered valid, and you must also protect this consent, along with the personal data.

Acceptance by clicking on a box, in which you expressly present the possibility of deciding whether or not to accept the data processing, is considered valid consent as long as you do NOT do so through pre-checked boxes.

Children's Consent

The collection, use and storage, i.e. the processing, of a child's personal data, requires their consent. Consent given by persons over 14 years of age is presumed valid, and for children under 14 years of age, it is necessary that their parents or guardians also give their consent. Remember to consult your DPO if you intend to collect data online from children, as you have to establish procedures so that parental consent can be verified.

5. Carrying out a Risk Analysis of the Processing of Personal Data, and if Necessary, an Impact Assessment

As a researcher, you have to assume responsibility by applying a level of security that is appropriate to the risk that the data may be accessed by unauthorized persons; altered or destroyed; or rendered inaccessible.

To do this, you have two tools: risk analysis (RA) and impact assessment. The UPV/EHU DPO who will advise you on performing these tasks.

DATA BREACHES	DAMAGE TO VALUES
Disclosure to unauthorized persons…	To confidentiality
Alteration, inaccuracy, manipulation…	To integrity
Loss, inaccessibility …	To availability

Risk Analysis (RA)

> The GDPR points out that measures to ensure compliance must take into account the nature, scope, context and purposes of the processing, as well as the risk to the rights and freedoms of individuals. According to this approach, some of the measures laid down by the GDPR will be applied only where there is a high risk to rights and freedoms, while others will have to be modulated according to the level and type of risk presented by the processing operations. (AEPD)

As the AEPD notes, you must, with your DPO's help, analyse the nature of your research, the context in which it is carried out and its purpose, to know the possible risks of a negative impact on the personal data you are processing, affecting the rights and freedoms of the people who have provided it. The three properties of the information you have collected that may be affected by an incident are:

1. **Confidentiality:** Property of the information to not be disclosed to unauthorized persons. Potential incidents: *Disclosure, theft*...
2. **Integrity:** Property of the information to not be altered and to retain its accuracy. Potential incidents: *Alteration, manipulation...*
3. **Availability:** Property of the information to be accessible to authorized persons. Potential incidents: *Inaccessibility, loss…*

The RA consists of analysing the probabilities that, at any given time, any of these three properties may be affected. You have to consider the hypothesis that unauthorised people will access your research data, that data will be mishandled accidentally or deliberately, or that you will not be able to access the research data because of an incident.

After determining these real possibilities (low/high risk), you have to assess what damage (mild/severe) it can cause to the rights of the donor persons if it occurs, and establish safety measures (simple/complex) depending on the level and type of risk.

At the UPV/EHU, the RA is carried out with the DPO before the processing is registered at the institution's ROPA, and takes into account the answers you provide about the means used in the processing and the security measures applied. It is important that the research teams are clear about:

1. The analysis of concrete scenarios of possible threats to the security of the personal data handled in your research. For example, regarding informed consent on paper that always contains the participant's signature, its loss or illegitimate use may facilitate impersonation of the participant in all forms of legal documents. Another source of incidents is sending information via unencrypted personal data to other members of the research team.
2. The use of UPV/EHU corporate computer equipment, which incorporates default security measures. If this is not possible, the equipment used must incorporate security measures equivalent to the equipment supplied by the institution.

Preparing a Data Protection Impact Assessment (DPIA)*

If, once performing the RA with your DPO, you conclude that the data processing you need for the research carries a significant or high risk for the rights of individuals, you will have to perform a data protection impact assessment (DPIA). That is, a systematic process with a specific methodology for analysing the significant risks that your research may entail for the protection of the data, and the rights and freedoms of the people who have donated them to you. The DPO usually has a model or program that facilitates this systematic process.

The DPIA is a tool for high-risk situations or when you use large amounts sensitive data (GDPR Article 35).

The objective of the DPIA is to determine: (a) the probability of undesired situations occurring, (b) the severity of their consequences, and (c) the mitigation measures needed to avoid or mitigate their consequences. In this way, you can establish the Initial Risk Level of the data

collection and use operations you have designed to carry out your research project, and the Acceptable Residual Risk Level once the containment or safety measures have been carried out.

With the DPIA, you can specify and describe the security or mitigation measures and the appropriate protocols you have initially foreseen for reducing, preventing and correcting the risks (probability and seriousness) at each key moment of the collection, use and retention of the data necessary for your investigation.

Recommendation or obligation of the DPIA: The DPIA is not always necessary, but it is recommended that, when considering each new collection and use of data, you perform an RA with your DPO to determine whether or not a DPIA is appropriate.

The DPIA is MANDATORY in research of the following types:

1. *High risk:* Collection, use and storage can pose a high risk to the rights and freedoms of individuals, e.g. people who have migrated for reasons of ideology or sexual identity.
2. *Systematic monitoring:* When personal information of natural persons is systematically collected and evaluated on the basis of automated processing, e.g. profiling.
3. *Use of privacy-invasive technologies:* The research project will use these:

    a) Drones.
    b) Data mining.
    c) Biometrics.
    d) Genetic techniques.
    e) Geolocation.
    f) Large-scale video surveillance.
    g) Electronic monitoring.

4. *Data processed on a large scale,* for example:

    - Requiring a large amount of data (volume, variety and duration or permanence of the data collection, use and storage activity).

MANDATORY DPIA

High-risk research, i.e. whether a processing activity is likely to result in a high risk for the rights and freedoms of natural persons, e.g. people who have migrated for reasons of ideology or sexual identity.

Research involves systematic monitoring; personal information is systematically collected and evaluated on the basis of automated processing, e.g. profiling.

Use of privacy-invasive technologies in research:

- Drones.
- Data mining.
- Biometrics.
- Genetic techniques.
- Geolocation.
- Large-scale video surveillance.

Research implies data processed on a large scale.

- On a regional or wider geographical scope (geographical extent of data collection, use and storage activity).
- Affecting large numbers of people (either in absolute terms or as a proportion of a given population).
- Refers to sensitive data such as biometrics, health, etc., and also includes personal data relating to children*.
- Where new technologies (which may have privacy risks) are applied on such a large scale.
- That they pose a high risk to the rights and freedoms of the persons concerned.

DPIA Contents[7]

The final result of the DPIA must be an Impact Assessment Report or a set of documents that adequately informs and reflects the characteristics of the processing assessed and the management of risks, i.e. the measures taken to mitigate them. This report, when available, will be collected with the rest of the documentation in your file of documentation on data protection in your specific investigation, provided to you by your DPO.

That IMPACT ASSESSMENT REPORT must include:

1. *Systematic description of the processing*: Detailing the categories of data you will collect, use and store; the people who will be able to access them; the information flow; and the technologies used (Chapter 1).
2. *Assessment of necessity and proportionality*: Discerns whether the purpose you are pursuing can be achieved by other means, for example by using other data or less data, by reducing the pool of donors quantitatively or qualitatively, by other less invasive technologies or by other procedures or means of treatment, etc. This judgment is based on three aspects to be reviewed once you have already worked on the first phase (Chapter 1):
    a) Adequacy: The data collected serve the purpose of the research.
    b) Necessity: There is no other more moderate way to perform the research with the same effectiveness.
    c) Proportionality: It is weighted or balanced, as more benefits or advantages for the general interest are derived than damage to other goods or values in conflict.
3. *Risk assessment:* Where you analyse the possible risks for the data protection of those concerned, which you have already established in the previous points that you will need, and you assess their probability and the impact of their materialisation.

[7] The AEPD has published on its website a guide for an Impact **Assessment on Personal Data Protection.** This is a very useful document for conducting a DPIA.

4. *Management of the risks:* include the measures you are to establish, as advised by your DPO, to deal with them.

Clearly, to perform a good DPIA and an adequate Report, the collaboration of the DPO (dpd@ehu.eus) is essential, both with active intervention in the design and execution of the evaluation, as well as in its coordination functions, main dialogue or collaboration with the evaluator.

In the UPV/EHU, the form with which you request the Data Protection Delegate to register the processing in the UPV/EHU ROPA evaluates, in function of the information you provide, the need for a DPIA. When the phrase 'AN IMPACT ASSESSMENT MUST BE MADE FOR THIS PROCESSING' appears below the estimated level of impact of the processing, it is mandatory that you respond to Section 16 of the form, which in itself constitutes a DPIA. But even better than all that is to rethink the ethical and methodological aspects that allow the research to be approached with a lower level of impact on the participants' privacy and rights. Many times, it is not possible, and it is then necessary to rethink the relevance of the methodology selected for research in the face of the risk it poses to the data subjects' privacy and rights.

Collection, Use and Data Retention (In The Cloud)

The use of online data processing such as cloud computing for research purposes requires good assessment and appropriate action:

- Assess the risks associated with handling such data in the cloud.
- Apply *risk minimisation measures* such as pseudonymisation or anonymisation, also if dealing with macrodata or Big Data[8].

[8] Big Data (macrodata): Comprised of the large amounts of data about our habits, schedules, etc., collected through devices (cell phones, sports bracelets, smart watches, computers, etc.) through which companies analyse sets of data, the data can be shaped or tested, trends can be sought, problem areas can be detected, etc. Normally, all data in Big Data are anonymised, so a particular person cannot be identified through that

- Gather and assess the conditions of the cloud service, its compliance with regulatory requirements (e.g. physical location of data, whether it is in legally secure space) and security measures (e.g. encryption of information in transit online).
- Sign a contract with the cloud service provider (when it is not the university) as it will have the status of 'processor', which includes that when the service is completed, the data will be returned to the researcher who has contracted the service.

data, but security measures have to be implemented to be applied so that anonymisation is not reversible. The anonymisation of personal data consists of limiting and eliminating the specific information that allows identification of the person concerned. The main objective is to avoid, in a definitive way, the re-identification of the person when the data are reused.

6. Ensuring Safety

GDPR Article 5.1.f establishes the need for you to ensure the appropriate security of the personal data, including protection against:

- unauthorised or unlawful processing
- accidental loss, destruction or damage.

To prevent this, you need to establish technical and organizational measures that ensure integrity, confidentiality and availability, but that also allow you to demonstrate (when required under supervision or audit) that you are implementing them during and after the investigation. Your DPO will advise you on all this.

Organisational Security Measures

Everyone on your research team needs to know that they have a duty of confidentiality that continues after the investigation is complete. They must also prevent access to the data by unauthorised persons. All those who will have access to the data should sign a confidentiality document.

To make those duties effective, you must implement the following organizational measures when designing the project:

1. It is advisable to adopt a set of security rules for the data processing and to make it known to your entire research team.

In our case, these rules must be compatible with the UPV/EHU Information Security Policy[9].

2. Roles and responsibilities, especially who will be responsible for security.
3. Management of computers, software, storage devices and network resources.
4. Training in day-to-day security measures:
   - Do not leave personal data exposed to third parties (unattended electronic screens, paper documents in publicly accessible areas, media with personal data, etc.);
   - Before leaving, lock the screen or close the session; store paper documents and electronic media in a secure place (cabinets or restricted-access rooms) 24 hours a day;
   - Do not communicate data or any personal information to third parties, especially during telephone consultations, e-mails, etc.
5. Secure procedures for access and response to the data subject whenever they want to exercise their rights: electronic means, referral to the IP, DPO, postal address, etc.
6. Protocol for action in the event of a security breach: In the event of improper access to personal data, alteration of information or loss of access, you must immediately contact your DPO to record the incident and evaluate its consequences. If the security breach may constitute a risk to the rights and freedoms of individuals, you must, without undue delay, inform them and the institution (UPV/EHU, in our case) through the DPO, notify the AEPD within a maximum of 72 hours, including all the information necessary to clarify the facts, through its electronic headquarters (https://sedeagpd.gob.es).

[9] Agreement of the 25th April 2013, from the Governement Council of the UPV/EHU by which it is approved the information segurity policy of the University of the Basque Country/ Euskal Herriko Unibertsitatea (UPV/EHU).

ORGANISATIONAL SECURITY MEASURES

- Adopt security standards for data processing equipment.
- Distribute roles: Especially who will be responsible for security.
- Organize the management of computers, software, storage devices and network resources.
- Comply with day-to-day security measures:
  1. Do not leave personal data exposed to third parties on unattended electronic screens, on paper documents in publicly accessible areas, on media with personal data, etc.
  2. Proceed to screen lock or logout before leaving.
  3. Always store paper documents and electronic media in highly secure places.
  4. Do not communicate data or any personal information to third parties, especially during telephone consultations, in emails, etc.
- Establish secure procedures for access and response to data subjects when they want to exercise their rights: electronic means, referral to the IP, DPO, postal address, etc.
- In the event of a security breach due to improper access, alteration of information or loss of access, contact your DPO immediately.

Technical Security Measures

Technical measures are elementary security measures for avoiding or minimizing risks, and that have to be periodically checked automatically (software or computer programs) or manually:

1. *Access control and authentication: Profiles and passwords:*
   a) Use several different profiles or users for each purpose: When you use the same computer or device for processing personal data from research and for other personal or professional use, it is recommended to keep these uses separate.

b) Provide profiles with administrative rights for installing and configuring the system and profiles of users without administrative privileges or rights for access to personal data: This measure prevents access privileges from being obtained or the operating system from being modified in the event of a cybersecurity attack.

c) Ensuring the existence of passwords for access to personal data stored in electronic systems, with at least 8 characters that are a mixture of numbers and letters.

d) Unequivocal identification: When different people will access the data, have a specific user profile and password for each person.

e) Passwords: You must guarantee the confidentiality of the passwords, avoiding their exposure to third parties. Under no circumstances may passwords be shared or left in a common place or accessed by persons other than the user.

2. *Access log file: Activity, monitoring and tracking:*

   a) The use of access log files is an important security measure that allows the identification and tracking of actions with personal data.

3. *Security of workstations, servers and networks:*

   a) Update: You have to ensure that you keep computers and devices updated as often as possible.

   b) Antivirus: The computers and devices on which you perform automated processing of personal data should have an antivirus system, and it should be updated regularly.

   c) Encryption: Network security is important both for external connections (e.g. to the Internet) and for interconnection with other systems (external or internal) within the university itself. When accessing via the Internet, encrypt the information with cryptographic protocols (TLS/SSL).

d) Firewall and intrusion detection: Monitor traffic to and from the information system with firewall and intrusion detection systems.

e) Segregation: the data network must be separated from the other networks.

4. *Data Encryption:*

   a) When you need to move personal data, whether by physical or electronic means, use a strong encryption method.

5. *Backup copies:*

   a) Periodically make a backup on a second medium different from the one you use for your daily work. Store the copy in a safe place, different from where you have located the computer with the original files, so you can recover your personal data in case of loss of information.

6. *Proper destruction of devices and deletion of data.*

7. *Physical security of the facilities.*

It is evident that all research groups to have to be formed and trained in this part of the tasks to carry out their projects. It is important to consider all this within the design of the research itself, as it requires time, work and human and material resources. Fortunately, your centre's DPO is always present to help you because it is their area of knowledge and competence.

TECHNICAL SECURITY MEASURES DURING THE RESEARCH

1. Access control and authentication: Profiles and passwords.
2. Access log file: Activity, monitoring and tracking.
3. Security of workstations, servers and networks:
    - Update.
    - Antivirus.
    - Encryption.
    - Firewall and intrusion detection.
    - Segregation of the data network from other networks.
4. Data encryption.
5. Backup copies.
6. Proper destruction of devices and deletion of data.
7. Physical security of the facilities.

7. Documenting Diligently

To complete the verification and control of this specific aspect of your research, it is necessary to prepare and keep a series of documents such as informed consents, the possible exercise of the data subjects' rights, incident management, signed confidentiality commitments, and if necessary, the data processors' contracts. There are documents that will be generated in the processing registration process or managed with your DPO that you do not need to store personally. The documents, how they are generated and who and where they should be kept are listed in the following sections.

1. Record of processing activities (ROPA).
2. Records of consents.
3. Registration of the exercise of rights.
4. Risk assessment.
5. Data protection impact assessment (DPIA).
6. Data breach register.
7. Confidentiality agreements or non-disclosure agreements.
8. Data processing agreement/contractual clauses for the transfer of personal data.
9. Appointment of the research project security manager.

All this documents won't be needed in all the investigations, but they are all the possible ones according to the Law.

Document 1. **Record of Processing Activities (ROPA)**

The ROPA is a mandatory document that lists the data processing activities carried out by the institution, including those corresponding to research projects. In our case, the ROPA is in electronic format and can be viewed on the UPV/EHU website (www.ehu.eus/babestu).

Once you have requested that the DPO register the data processing associated with your research, it will be included in the ROPA (of the UPV/EHU or the corresponding institution). It is not necessary, although convenient, that you keep a list of the treatments you have in your ROPA.

The information contained in the ROPA of your treatment is that corresponding to the second layer of information.

Document 2. **Record of Consents**

As the responsible PI, you must have saved, in electronic or paper format, all the subjects' consents for the processing of their data. These documents will allow you, if necessary, to prove the legitimacy of the processing. Whether in paper or electronic format, you must keep them securely in a location you will have to detail in the processing declaration form. Your DPO will advise you on how to do this as well.

Document 3. **Registration of the Exercise of Rights**

The people participating in your research can exercise their AREOPL rights through the DPO (of the UPV/EHU, in our case). When they contact the PI or any member of the research team, the DPO must be informed immediately and will keep a record of all requests for rights received and the responses given to them. This record will be located at the same email address provided to you by the DPO at the time of the recording of the treatment.

Document 4. **Risk Assessment**

The RA report must be kept up to date and must document the RA performed, its conclusions and the security measures taken. This document is also incorporated prior to the registration of the treatment in the ROPA and is located in the platform or file assigned to you by the DPO.

Document 5. **Data Protection Impact Assessment (DPIA)**

In research projects with high risk or with massive processing of specially protected data, this report or reports are mandatory (if they have to be reissued due to changes in the research project).

This document is included in the treatment declaration form and is incorporated prior to recording the treatment in the ROPA assigned to you by the DPO.

Document 6. **Incident Management Record**

When a situation occurs that affects personal data, you should contact your DPO, who should record the incident, and if necessary, notify the AEPD.

It is advisable to keep a record of such incidents with a description of each one, the data and persons affected, the consequences and the measures taken. This record is located at the same e-mail address or platform assigned to you by the DPO at the time you registered the data processing when designing your investigation.

Document 7. **Confidentiality Commitments**

You will have saved, in electronic format (requires an electronic signature) or on paper, all the confidentiality agreements signed by the people who access the personal data of your research. These documents are also located at the same electronic address or platform provided to you by the DPO at the time of registration of the processing.

Document 8. **Data Processing Agreements**

Processor contracts, if any, must be signed and saved in electronic format (electronic signature required) or on paper. An official model contract is available from our institution (www.ehu.eus/babestu)[10]. Like the rest of the documentation, they must be collected on the platform or e-mail address provided by your DPO.

Document 9. **Appointment of the Research Project Security Manager**

It is advisable to appoint a team member as security manager and to reflect this in a document indicating who it is and how they have accepted and understand their responsibilities. As with the rest of the documentation, this appointment must be reflected in the platform or e-mail address provided by your DPO.

[10] «Commitments to asume by external enterpraises who develop data treatment on behalf of the UPV/EHU», aproved by the Council of Government in the 10th of April of 2008 session.

8. Apendix

Informed Consent to Request Participation in Research and the Use of Samples or Data

To carry out scientific research involving human beings, either in person or with their samples or data, it is obligatory that there is a free and deliberate expression of will to participate, validly issued by capable persons, or their authorised representatives, preceded by appropriate information (LIB Article 3(f))[11].

To arrive at such a statement, each participating subject must be adequately informed about the research, and only then can they decide. In the case of requesting their data, specific information about it must be included, and in addition to the collection of consent to be a participant in research, a specific section for collecting consent for the use of personal data must be included, as required by current regulations.

[11] Spanish Biomedical Research Act —Ley de Investigación Biomédica LIB—.

BASIC STRUCTURE OF AN INFORMED CONSENT DOCUMENT

INSTITUTIONAL LOGO (UPV/EHU in our case)

RESPONSIBLE RESEARCHER IDENTIFICATION

- Name and Surname.
- Department and Centre.
- Contact details: Institutional email address and telephone number.

RESEARCH BRIEF (Minimum mandatory information)

- Project identification: Title and financing.
- Brief summary of the project:
  - — Objectives and expected benefits.
  - — Duration.
  - — Place of performance.

DESCRIPTION OF THE INTERVENTIONS to be carried out on the subject recruited:

- Type and description of the test or intervention (survey, sampling, audio recording, video...) and its objective.
- Number of times it will be performed, dates and deadlines.
- If there is to be further contact with the participant.
- Description of risks and/or inconveniences and measures to minimize them (including insurance if applicable).
- Offer to clarify doubts, provide more information and contact details.

VOLUNTARINESS

The person decides whether or not to participate. They are informed that participation is voluntary and that refusal to do so will not result in any harm or action against them.

WITHDRAWAL

The person is informed that they may withdraw from the investigation at any time without personal consequences and without the need to give any explanation. They are also informed of who to contact (PI) and the institutional contact address to make the withdrawal effective.

SAMPLE DESTINATION

Information is given so that the concerned person can decide what can be done with their samples after the investigation has been completed:

- Destruction.
- Anonymization.
- Free transfer to Biobank, identifying it.
- Conservation in sample collection for research related to the initially proposed study.
- Other destination.

PROTECTING YOUR DATA

When the subject provides personal data, they are informed that, in accordance with the General Data Protection Regulation (EU2016/679):

The personal data requested are . . . . . .
The data processing code is . . . . . .
The data processing is . . . . . .
The purpose of this treatment is . . . . . .
The data controller is . . . . . .

In our case, it will be the UPV/EHU: Universidad del País Vasco/Euskal Herriko Unibertsitatea CIF: Q4818001B; postal address: Barrio Sarriena s/n, 48940-Leioa (Bizkaia); website: www.ehu.eus; contact details of the Data Protection Officer (dpd@ehu.eus)

The period of data storage data will be . . . . . .

The legitimacy of the processing is the subject's informed consent.

Possible international transfers of data indicating whether and to whom they will be transferred.

Transfer

NO: 'This information may not be accessed by any person outside the project, except in compliance with a legal obligation.'

YES: 'The information you provide will be accessible by other researchers or universities, specifying to whom and why.'

International data transfers

NO: 'The data will not be transferred to other countries outside the European Union.'

YES: 'The data will be transferred to other countries outside the European Union.'

The rights on your data which are those of access, deletion, rectification, opposition, limitation of processing, portability and oblivion.

In our case you can exercise them by sending your petition to HYPERLINK “mailto:dpd@ehu.eus” dpd@ehu.eus. You can find all the aditional informatio in HYPERLINK “http://www.ehu.eus/babestu” http://www.ehu.eus/babestu The complete information about this treatment is in: https://www.ehu.eus/es/web/idazkaritza-nagusia/ikerketa-datu-pertsonalen-tratamenduak

Destination of the data: Information is provided on what will be done with the data transferred for the research, once it is concluded:

- Destruction.
- Anonymization.
- Transfer, identifying to whom.
- Storage for research related to the initial proposal.
- Other destination.

GRATUITY

The subject concerned is informed that participation by providing their data, samples, answering surveys, etc., is altruistic and therefore there will be no remuneration for it. If there is compensation, it will be described.

ACCESS TO RESEARCH FINDINGS

The subject is informed that they can learn the results of the research by contacting the person responsible for the research.

In the case of genetic data, information is given on the possibilities:

- Possible unexpected discoveries.
- Right not to know.
- Information to relatives.
- Genetic counselling.

CONSENT SIGNATURES FOR PARTICIPATING IN THE RESEARCH

- Identification, date and signature of the person in charge of informing and collecting the Consent Document.
- Identification, date and signature of the person who gives consent to participate in the research.
  - — Under 12 years old: Identification and signature of the legal representative.
  - — Over 12 years old and up to 18 years old: Identification and signature of consent of the legal representative and identification and proof of assent of the minor.

DATA PROCESSING CONSENT SIGNATURES

- Identification and signature of the person who consents to the use of their personal data under the conditions described in the PROTECTION OF YOUR DATA section of this document:
  - — For children under 12: Signature of legal representative.
  - — For data from children who are 12 years old and under 14 years old: Signature of the legal representative and proof of the child's consent.
  - — For data from children aged age 14 and above: Signature of the child.
  - — For data from children under 18 years of old in an invasive investigation (psychological risk during collection): Signature of the legal representative and proof of the child's consent.

Koadernoak
Cuadernos
Notebooks

IKERKETA
ERRETOREORDETZA
VICERRECTORADO
DE INVESTIGACIÓN

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea