PRIBATUTASUNA DISEINUTIK ETA MODU LEHENETSIAN BERMATZEKO POLITIKA

ZIURTAPEN ETA
ZERBITZU
ENPRESA-EMPRESA
DE CERTIFICACION
Y SERVIC

Beato Tomás de Zumárraga
71 - 1ª Planta
01008
Vitoria - Gasteiz

www.izenpe.eus
izenpe@izenpe.eus

Edukia

1. Kontroleko informazioa.

Laburpena

MOTA	Politika
EREMUA	Pribatutasuna, segurtasuna
IZENBURUA	Pribatutasuna diseinutik eta modu lehenetsian bermatzeko politika

Bertsioen historia

BERTSIOA	DATA	EGILEA	ALDAKETAK
1.0	2024/02/22	Segurtasunaz arduratzen den zerbitzua Datuak Babesteko Ordezkaria	

Onarpenen kontrola

BERTSIOA	AURKEZTUA	BERRIKUSPENA	ONARPENA
1.0	Segurtasunaz arduratzen den zerbitzua Datuak Babesteko Ordezkaria.		Segurtasun Batzordea

1. Sarrera

Datu pertsonalen babeserako araudiak zenbait neurri hartzera behartzen ditu erakunde guztiak, Ziurtapen eta Zerbitzu Enpresa–Empresa de Certificación y Servicios, Izenpe, SAk (aurrerantzean, «Izenpe») dauzkan datu pertsonalen segurtasuna, osotasuna eta konfidentzialtasuna bermatzeko, baita haien kontsulta, tratamendu, lagapen, biltegiratze eta ezabatze egokia bermatzeko ere.

Indarrean dagoen Datuen Babeserako Erregelamendu Orokorrak, 2016ko apirilaren 27koak (aurrerantzean, «DBEO»), datu pertsonalen babesari buruzko araudi nazionalak eta beste edozein legeria aplikagarrik beharrezkotzat jotzen dute arlo honetan segurtasun-neurriak ezartzea; aurrea hartzen diete erakunde modernoek bete behar dituzten baldintza teknologiko berriei, eta datu pertsonalak tratatzen dituzten erakundeek zer norabideri jarraitu behar dioten adierazten dute.

Erantzukizun proaktiboaren printzipioa (*accountability*) eta haren ezarpena ahalbidetzen duten tresnak lotzeko beharrak , bidea ematen dio pribatutasuna diseinutik bermatzeko printzipio galdagarriari (*Privacy by Design*), baita beste tresna batzuen erabilerari ere; esaterako, eraginaren ebaluazioa, bere ingelesezko izenagatik ezaguna, *Privacy Impact Assessment* edo PIA (zeina arlo honi buruzko beste prozedura espezifiko baten xede baita).

S. Garre Guik dioenaren arabera1, pribatutasuna diseinutik eta modu lehenetsian bermatzea eta eraginaren ebaluazioak erabiltzea berez arlo teknologikoetakoak diren metodologietatik ondorioztatzen dira; horri esker, datu pertsonalak tratatzea dakarren edozein ekimenek pribatutasunean duen eragina ebaluatzen da, bereziki sorreraren hasierako egoeretan, Izenpek dituen datu pertsonaletan eragina izan dezaketen edo haiek arriskuan jar ditzaketen ondorio posibleak saihesteko edo murrizteko beharrezko neurriak hartu ahal izan daitezen.

Komeni da aipatzea, kostu ekonomikoak murriztearen ikuspegitik, askoz ere baliagarriagoa dela gainbegiratze-metodologia jarduera sortzen denetik txertatzea, datu pertsonalak tratatzeko tresna automatizatuak, aplikazio informatikoak, jarduera-programak edo beste edozein eratakoak erabiliz, eta ez sortu eta gauzatu ondoren baloratzea legezkotasunaren ikuspegitik dituen eragozpenak eta, gero, dena berregin behar izatea.

Horri dagokionez, Datuak Babesteko Espainiako Agentziaren arabera, «informazio pertsonalak gero eta balio ekonomiko handiagoa du, eta, hori dela eta, ezinbestekoa da planteamendu tradizionalak beste batzuekin osatzea; hain zuzen ere, pertsonen eskubideak errespetatzen eta bezero eta erabiltzaileen konfiantza indartzen laguntzen duten ikuspegi proaktibo berriekin».

Horrek ez du inola ere esan nahi alde batera utzi behar denik lege-mailako xedapenak betetzeko eskakizunean oinarritutako ikuspegia; aldiz, betetzen direla bermatzeko, gero eta beharrezkoagoa da prestasunez jokatzea eta konpromiso arduratsua hartzea arriskuak saihesteko edo minimizatzeko halakoak gertatu aurretik.

Izenpen erantzukizun proaktiboa sendotzeko bidean, bereziki baliagarriak dira pribatutasuna diseinutik bermatzea eta antzeko beste ikuspegi batzuk; ikuspegi horrek defendatzen du hasierako fasetik hartu behar direla kontuan datuak babestearen eta pribatutasunaren auziak, produktu edo zerbitzu bat diseinatzen den unetik beretik.

---

[1] S. Garre Gui, *Introducción a la seguridad de la información*. Ed. Fundación UOC, Bartzelona, 2006.

Horrela, askoz ere eraginkortasun handiagoz babesten dira kaltetuen eskubideak, eta maizegi gertatzen den zerbait ere saihesten da: araua *a posteriori* egokitzea teknologiara, garatu edo ezarri ondoren ikusten delako haren irregulartasuna, kostu handiak baititu hura berriro diseinatu eta egokitzeak (Datuak Babesteko Espainiako Agentziaren Datu Pertsonalak Babestearen Eragina Ebaluatzeko Gida).

2. Helburua.

Politika honen helburua da portaerazko jarraibideak ezartzea datu pertsonalak tratatzea dakarren edozein ekimenek pribatutasunean eta tratamenduan duen eragina ebaluatzeko, bereziki sorreraren hasierako egoeretan, Izenpek dituen datu pertsonaletan eragina izan dezaketen edo haiek arriskuan jar ditzaketen ondorio posibleak saihesteko edo murrizteko beharrezko neurriak hartu ahal izan daitezen.

Politika honek Izenpen ezarrita dauden eta erabat indarrean dauden segurtasuneko eta arauak betetzeko neurri guztiak osatzen ditu.

3. Jardun-eremua eta helmena.

Izenpe osoari aplikatzen zaio politika, eta haren eremu guztietara iristen da. Bereziki, sailetako arduradun guztiek hartu behar dute kontuan, eta barneko edo kanpoko ekimen orotan gorde behar da, datu pertsonalak tratatzea dakarren edozein eratako prozesu bat diseinatzeko ekintza edo proiektuetan; besteak beste, zerbitzuak, produktuak, programak edo euskarri informatikoak, gailuak, aplikazioak edo antzeko beste edozein ekimen garatzean.

4. Politika aplikatzeko printzipioak eta eragindako langileak.

Politika hau Izenpen dagoen informazio pertsonalaren segurtasuna, osotasuna eta konfidentzialtasuna bermatzera bideratutako printzipio batzuetan oinarritzen dira. Printzipio horiek hor egon behar dute ezarri nahi den ekimena kudeatzeko uneetan; gero ere gorde behar dira, eta ez dira iraungiko.

Hauek dira printzipio horiek:

- Proaktibitatearen printzipioa. Legezkotasuna eta segurtasuna gordetzea, ekimena ezarri aurretik, haren bizitza baliagarrian zehar eta erakundetik desagerrarazten den arte, eta legean ezarritako neurriak hartzea.
- Pribatutasun lehenetsiaren printzipioa. Segurtasuna datu pertsonalak tratatzea dakarren erakundeko edozein jarduera sortzeko estandar gisa hartzea. Erakundearekin harremanetan dagoen jendeari informazio pertsonala segurtasunez eta konfidentzialtasunez tratatzen dela jakinarazteko modua.
- Pribatutasuna diseinutik bermatzeko printzipioa. Datuak babesteko ordezkariak hor egon behar du edozein ekimen sortzean, legezkotasuna eta segurtasuna gorde daitezen ekimena kudeatzeko prozesuan, erakundeari denbora eta dirua aurrezten laguntzeko eta amaituta edo ezarrita egotean ekimena berregin behar ez izateko indarreko legezkotasuna betetzen ez duelako.
- «end to end» segurtasun-printzipioa (muturretik muturrerako printzipioa edo hasieratik amaierarako printzipioa). Prozesuko etapa guztietan egon behar du bermatuta segurtasunak, baita funtsezko aldaketetan ere, esklusiorik eta salbuespenik gabe.

Ezaugarri hauek dituzte prozedura horiek:

- Eragina baloratzeko metodologiak sistematikoa eta erreproduzigarria izan behar du, emaitza gisa datu pertsonalen tratamenduaren segurtasun iraunkorra izango duten prozesuak berrikusteko.
- Ekimenaren funtzionalitatea, erabilerraztasuna eta konfiguragarritasuna prozesuari lotuta daude, eta kontuan hartu behar dira, oreka egokiaren bila.
- Ekimena askotariko plataformetan eskuragarri egoteak ez ditu ahuldu behar deskribatutako printzipioak, erakundearen irudia eta fidagarritasuna konprometitzen baititu harekin harremanetan dagoen jendeari dagokionez.

5. Eragindako langileak.

Nahitaez, datu pertsonalak tratatzea dakarren edozein ekimen sortzean, erabakitzeko gaitasuna duten profilek parte hartu behar dute, datuak babesteko ordezkariak gainbegiratuta; adibidez:

- Departamentu juridikoko arduraduna;
- ITen/Sistemen arduraduna, eta
- Eragindako sailen arduraduna

Azken beltzean, proiektua kudeatzean, hautematen arriskuen deskribapena, haiek saihesteko ezarritako segurtasun-neurriak, jarraipen-neurriak, eta beharrezko datu pertsonalak soilik tratatzen direla ziurtatzeko eta aurreikusitako eta zehaztutako xedeetarako ezarriko diren kontrolak. Azken emaitzaren dokumentuak aurretik zehaztu behar diren gutxieneko edukia eta egitura izan behar ditu.

6. Metodologia.

Politika honen bidez, tratatu behar diren datu pertsonalen segurtasuna eta pertsonen funtsezko eskubideak bermatzeko DBEOn jasota dagoen agindua betetzeko prozesua ezartzeko metodologia biltzen da: «Tratamenduaren nolakotasuna, eremua, testuingurua eta helburuak kontuan hartuta, bai eta pertsona fisikoen eskubide eta askatasunetarako dauden askotariko probabilitate eta larritasun-mailako arriskuak ere, tratamenduaren arduradunak arrazoizko neurri tekniko eta antolakuntzakoak hartuko ditu, tratamendua erregelamendu honekin bat datorrela bermatzeko eta frogatu ahal izateko. Neurriok beharrezkoa denean berrikusi eta eguneratuko dira.» (DBEOren 24.1 art.).

Segurtasun-arduradunak eta datuak babesteko ordezkariak ziurtatuko dute, metodologia hori aplikatuz, bermatuta geratuko dela Izenpen ez dela ezarriko honelako prozesuak:

- Tratamenduaren xedeetarako beharrezkoak ez diren datu pertsonalak tratatzen badituzte (tratatutako datuen mugapena);
- Prozesu berrian, ez dira tratatuko datuak aurreikusitakoak ez diren xedeetarako (xedearen mugapena);
- Analisian, datuen erabilera denboran mugatzen badute, behar baino luzaroago tratatu ez daitezen (kontserbazio-denboren mugapena); eta

- Datu pertsonalak tratatu behar ez dituztenek haietarako sarbidea izan dezaten saihestea (sarbidearen mugapena).

Pribatutasuna diseinutik eta modu lehenetsian bermatzeko politika hau ezartzeko, baliteke eraginaren ebaluazioa egin behar izatea (prozedura espezifiko baten bidez), datu pertsonalak tratatzen badira eta ondorioz arriskuan jartzen badira pertsonen eskubideak edo datu pertsonalen segurtasuna.

7. Gorabeherak jakinaraztea.

Politika hau ezartzean edo proposatutako metodologia aplikatzeko edozein fasetan gertatzen den gorabehera esanguratsu oro segurtasun-arduradunari edo datuak babesteko ordezkariari jakinarazi beharko zaio, balora dezan eta horren arabera jardun dezan.

8. Aurretiko kontsulta.

Politika hau aplikatzea dela bide prozesu, produktu edo zerbitzu berri bateko analisi ororen ondorioek arrisku nabarmenean jarriko balituzte datu pertsonalak edo interesdunen eskubideak, kontsulta egingo zaio kontrol-agintaritzari datu pertsonalak tratatu baino lehen. Horrela jokatuko da 35. artikuluaren arabera datuak babesteari buruzko eraginaren ebaluazio batek erakusten badu tratamenduak arrisku nabarmena eragingo lukeela arduradunak neurririk hartzen ez badu hura arintzeko.