



6.3 Datu pertsonal eta pribatasunaren babesa

Gaur egun, **datu pertsonalen babesa eta pribatutasuna bermatzea funtsezkoa** da, informazioaren gizartean bizi garen heinean. Segurtasun digitalak gure **datuak modu arduratsu eta seguruan kudeatzea** eskatzen du, batez ere online plataformetan. Horrek esan nahi du datuak partekatzearen arriskuak ulertzea, pribatutasuna babesten duten legeak ezagutzea (DBEO) eta datu pertsonaletara sarbidea duten pertsonak kontrolatzea.

Datu pertsonalak babestea bermatzeko hainbat esparrutan aplikatu beharreko neurriak daude. **Hezkuntza-arloan**, ikasleek beren datuak eskolako plataforma digitaletan nola partekatu behar dituzten jakin behar dute. Horretarako, informazio pertsonala babesteko modurik seguruena aukeratzea, eduki egokiak eta desegokiak bereiztea, eta beren datuak nola erabiltzen diren ebaluatzeko gaitasuna izatea funtsezkoa da.

Lan-munduan ere, datu pertsonalen babesa garrantzitsua da. Merkataritza, marketina, osasungintza eta irudi pertsonala bezalako sektoreetan, enpresaren webgunean edo sare sozial korporatiboetan partekatzen den informazioa arduraz kudeatu behar da. Gainera, Datuak Babesteko Europako Erregelamendu Orokorra (DBEO) eta "ahazteko eskubidea" kontuan hartu behar dira.

Datu pertsonalen babesa eta segurtasun digitala

Adimen artifizialaren (AA) garapenak ere datu pertsonalen erabilera berriak ekarri ditu. Adibidez, laguntzaile birtualekin egindako ahots-interakzioak datu pertsonaltzat hartzen dira eta DBEOren arabera babestu behar dira. Hirugarrenei datu pertsonalak kudeatzeko baimena eman aurretik, horrek ekar ditzakeen onurak eta arriskuak aztertu behar dira. Gainera, AA sistemetan segurtasun-neurriak ezartzea garrantzitsua da, hala nola datuen anonimizazioa, zifratzea edo izenordeekin lan egitea.

Datu-analisisa ere datu pertsonalen babesean zuzenean eragiten duen alor bat da. Big Data teknikak aplikatzean, informazio pertsonala bildu eta biltegitartzeko arriskuak identifikatu behar dira. Hori dela eta, DBEOren araudia ezagutzea eta baimenik gabeko sarbideen aurkako babes neurriak ezartzea ezinbestekoa da.

Bestalde, **cloud-sistemek** gero eta zabalpen handiagoa dute, baina horiek erabiltzean, pribatutasuna bermatzeko hainbat neurri hartu behar dira. Cloud plataformak aldizka ikuskatzea, datuak atzitzeko politikak ezartzea eta pribatutasun-estandar altuak betetzen dituzten hornitzaileekin lan egitea gomendagarria da. Gainera, erakundeek segurtasun-kultura bat sustatu behar dute langile eta erabiltzaileen artean.

Enpresetan, datu pertsonalen babesa bermatzeko **politika** argiak ezarri behar dira. Politika hauek datuen bilketa eta tratamendua, sarbide kontrolak, kontserbazio eta



ezabatze prozedurak, eta interesdunek beren datuak eskuratzeko, zuzentzeko eta ezabatzeko duten eskubidea arautu behar dituzte. Horrez gain, enpresetako langileei datuen babesari buruzko prestakuntza eta sentsibilizazio saioak ematea ezinbestekoa da.

Ondorioa

Datu pertsonalak helburu jakin eta legítimoekin soilik erabiliko direla bermatu behar da. Informazioaren erabileran arduraz eta erantzukizunez jokatu behar da, pribatutasuna arriskuan jartzen duten praktikak saihestuz. Gainera, erabiltzaileen baimen esplizitua lortzea eta datuen erabilera arautzen duten enpresen politikak definitzea funtsezkoa da. Gaur egungo testuinguru digitalean, segurtasun digitalerako jarrera proaktiboa izatea eta pentsamolde kritikoa garatzea ezinbestekoa da.

(azken eguneratzea: 2025/05/20)

Eusko Jaurlaritzaren Lanbide Heziketako Sailburuordetza. Lan honek Creative Commons Aitortu-EzKomertziala-PartekatuBerdin 4.0 Nazioarteko Baimena dauka (CC BY-NC-SA 4.0).

