

DIPUTACIÓ DE VALÈNCIA



Protecció de Dades i Seguretat de la Informació



QUADERNS DIVALDATA

Quaderns dirigits a delegats,
responsables i especialistes en protecció

.

Quadern nº 30 | Desembre 2022

ANONIMITZACIÓ DE DADES PERSONALS



Í N D E X



ANONIMITZACIÓ DE DADES PERSONALS

	Pàgina
Introducció	2
Conceptes bàsics d'anonimització de dades	3
El procés d'anonimització	4
Tècniques bàsiques d'anonimització	5
k-anonimat	7
Material complementari i notícies	8



Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interès per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades i Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUBSCRIPCIONS

Si desitges subscriure't a la nostra publicació accedeix al següent

[enllaç](#)



***“SENT CONSTITUTIVA D'INFRACCIÓ
MOLT GREU LA REVERSIÓ DELIBERADA
D'UN PROCEDIMENT D'ANONIMITZACIÓ
A FI DE PEREMITIR LA REIDENTIFICACIÓ
DELS AFECTATS”.***

INTRODUCCIÓ

Recentment l'Agència Espanyola de Protecció de Dades (d'ara en avant, “AEPD”) ha publicat una traducció de la “Guia bàsica d'anonimització” elaborada per l'Autoritat Nacional de Protecció de Dades de Singapur (Personal Data Protection Commission – PDPC) donada la seua especial rellevància per a responsables, encarregats de tractaments i delegats de protecció de dades.

La guia té per objectiu proporcionar orientacions sobre com realitzar de forma adequada l'anonimització bàsica i la desidentificació de conjunts de dades estructurades, textuais i no complexos.

El Reglament General de Protecció de Dades estableix, en el seu article 32, com a mesures per a garantir un nivell adequat al risc, la seudonimització i el xifratge de dades personals. És per això que l'anonimització i seudonimització de la informació de caràcter personal permet la protecció de les dades personals dels interessats si es realitza de manera adequada, sent constitutiva **d'infracció molt greu** “la reversió deliberada d'un procediment d'anonimització a fi de permetre la reidentificació dels afectats” (article 72 Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals).



CONCEPTES BÀSICS D'ANONIMITZACIÓ DE DADES

Per a abordar-la la citada Guia, és necessari partir dels conceptes centrals:

- **Anonimització:** procés que consisteix en la conversió de dades personals en dades personals que no es poden utilitzar per a identificar a cap individu. L'anonimització s'ha de considerar com un procés basat en risc, que inclou tant l'aplicació de mesures tècniques d'anonimització com a salvaguardes per a evitar la reidentificació.
- **Desidentificació:** es basa en l'eliminació d'identificadors (com ara: nom, adreça o número de DNI) que identifiquen directament a un individu. En la Guia s'incideix en què se sol equiparar erròniament a l'anonimització. No obstant això, és necessari aclarir que la desidentificació és només el primer pas de l'anonimització. Un conjunt de dades desidentificat pot tornar a identificar-se fàcilment.
- **Reidentificació** es refereix a la identificació dels particulars a partir d'un conjunt de dades que prèviament va ser desidentificat o anonimitzat.

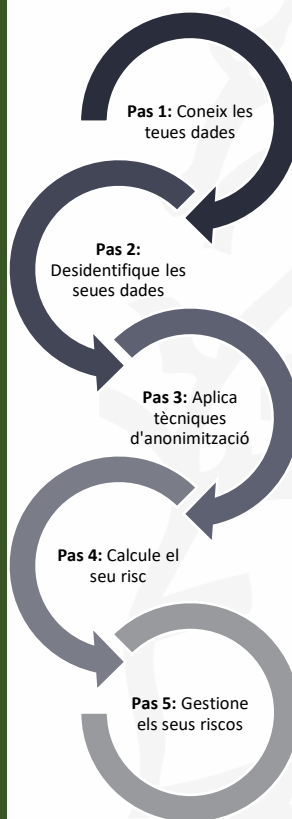
Les dades anonimitzades no es consideren dades personals i, per tant, no els resulta d'aplicació la normativa de protecció de dades. En aquest sentit s'estableix el Considerant 26 del RGPD.

***“L'ANONIMITZACIÓ S'HA DE
CONSIDERAR COM UN PROCÉS BASAT
EN RISC, QUE INCLOU TANT
L'APLICACIÓ DE MESURES TÈCNIQUES
D'ANONIMITZACIÓ COM A
SALVAGUARDES PER A EVITAR LA
REIDENTIFICACIÓ”***



EL PROCÉS D'ANONIMITZACIÓ

**“PER A DESIDENTIFICAR LES DADES ÉS
NECESSARI ELIMINAR TOTS ELS
IDENTIFICADORS DIRECTES”.**



En la Guia es presenten cinc passos per a anonimitzar els conjunts de dades quan siga apropiat.

Un registre de dades personals es compon d'atributs de dades que tenen diversos graus d'identificabilitat i sensibilitat a un individu. Per exemple: els “identificadors directes” són atributs que són exclusius d'un individu i es poden usar com a atributs de dades clau per a tornar a identificar a l'individu.

Per a desidentificar les dades, és necessari eliminar tots els identificadors directes (per exemple, els noms).

Opcionalment, es pot assignar un pseudònim a cada registre si és necessari vincular el registre a un individu únic.

En el següent pas, s'aplicaran tècniques d'anonimització dels identificadors indirectes perquè no es puguin combinar fàcilment amb altres conjunts de dades que puguin contindre informació addicional per a tornar a identificar a les persones.

En abordar el pas 4, en la Guia s'esmenta el mètode k-anonimat per a calcular el nivell de risc de reidentificació d'un conjunt de dades.



***“LA SEUDONIMITZACIÓ S'UTILITZA
QUAN ELS VALORS DE LES DADES HAN
DE DISTINGIR-SE DE MANERA ÚNICA I
NO ES CONSERVA CAP CARÀCTER O
QUALSEVOL ALTRA INFORMACIÓ
IMPLÍCITA SOBRE ELS IDENTIFICADORS
DIRECTES DE L'ATRIBUT ORIGINAL”.***

TÈCNIQUES BÀSIQUES D' ANONIMITZACIÓ

En l'Annex A de la citada Guia s'inclou un catàleg de tècniques bàsiques d'anonimització de dades:

- **Supressió de registres:** es refereix a l'eliminació d'un registre complet en un conjunt de dades. Aquesta tècnica afecta a múltiples atributs al mateix temps. L'eliminació ha de ser permanent i no sols una funció de “ocultar fila”.
- **Emmascarament de caràcters:** es refereix al canvi dels caràcters d'un valor de dades. Pot realitzar-se mitjançant l'ús d'un símbol (per exemple “*” o “x”). Habitualment l'emascarament s'aplica solament a alguns caràcters d'un atribut. Aquesta tècnica se sol utilitzar quan el valor de les dades és una cadena de caràcters i ocultar part d'ella és suficient per a proporcionar el grau d'anonimat requerit.
- **Seudonimització (o “codificació”):** consisteix en la substitució de dades d'identificació per valors inventats. Els pseudònims pot ser irreversibles quan els valors originals s'eliminen correctament i la seudonimització es realitza d'una manera no repetible. Aquesta tècnica s'utilitza quan els valors de les dades han de distingir-se de manera única i no es conserva cap caràcter o qualsevol altra informació implícita sobre els identificadors directes de l'atribut original.
- **Generalització:** es basa en la reducció deliberada de la precisió de les dades. Un exemple d'aquesta tècnica consistiria a convertir l'edat d'una persona en un rang d'edat. Normalment s'utilitza aquesta tècnica per a supòsits en els quals la generalització permet que la informació resultant continue sent útil per al propòsit previst.
- **Intercanvi:** aquesta tècnica – que també es coneix com remenat i permutació – consisteix a reorganitzar les dades en el conjunt d'informació de manera que els valors dels atributs individuals seguisquen representats en el conjunt de dades, però generalment no responen als registres originals.
- **Pertorbació de dades:** mitjançant aquesta tècnica els valors del conjunt de dades original es



***“MITJANÇANT LA TÈCNICA DE
PERTORBACIÓ DE DADES ELS VALORS
DEL CONJUNT DE DADES ORIGINAL ES
MODIFIQUEN PERQUÈ SIGUEN
LLEUGERAMENT DIFERENTS”.***

modifiquen perquè siguen lleugerament diferents. Se sol utilitzar per a identificadors indirectes (normalment números i dates), que poden ser potencialment identificables quan es combinen amb altres fonts de dades, però els canvis lleus en el valor són acceptables per a l'atribut. Aquesta tècnica no ha d'utilitzar-se quan la precisió de les dades siga crucial.

- **Agregació de dades:** consisteix en la conversió d'un conjunt de dades d'una llista de registres a valors resumits. Se sol utilitzar quan no es requereixen registres individuals i les dades agregades són suficients per a la finalitat.



***“SEMPRE QUE SIGA POSSIBLE, HA
D'ESTABLIR UN VALOR DE K-
ANONIMAT MÉS ALT (PER EXEMPLE, 5
O MÉS) PER A L'INTERCANVI DE DADES
EXTERNES ”***

K-ANONIMAT

k- anonimat és un model utilitzat per a garantir que no s'haja superat el llindar de risc, com a part de la metodologia d'anonimització.

S'utilitza per a confirmar que les mesures d'anonimització implementades aconseguixen el llindar desitjat contra els atacs d'enllaç.

A aquest efecte, s'entén com a “llindar de risc” el nivell de risc que l'entitat està disposada a tolerar.

El model k-anonimat s'utilitza com a guia abans que s'hagen aplicat tècniques d'anonimització (per exemple, generalització), i per a la verificació posterior també, per a garantir que els identificadors indirectes de qualsevol registre siguen compartits per almenys k-1 altres registres. Per tant, no és possible vincular o assenyalar el registre d'un individu, ja que sempre hi ha k atributs idèntics.

A més, en la Guia s'afeg la següent nota respecte a la k-anonimat:

“Sempre que siga possible, ha d'establir un valor de k-anonimat més alt (per exemple, 5 o més) per a l'intercanvi de dades externes, mentre que es pot establir un valor més baix (per exemple, 3) per a l'intercanvi de dades internes o la retenció de dades a llarg termini.

No obstant això, si no pot anonimitzar les seues dades per a aconseguir-ho, ha d'implementar mesures de seguretat més estrictes per a garantir que les dades anonimitzades no es divulguen a parts no autoritzades i es mitiguen els riscos de reidentificació.

Alternativament, pot contractar experts perquè proporcionen mètodes d'avaluació alternatius per a aconseguir riscos de reidentificació equivalents.”



MATERIAL COMPLEMENTARI

- Guia bàsica d'anonimització. Elaborada per Autoritat Nacional de Protecció de Dades de Singapur. Consulta [aquest enllaç](#).
- Directrius d'assessorament del PDPC sobre la Llei de Protecció de Dades Personals per a Temes Seleccionats. Consulta [aquest enllaç](#).
- Nota tècnica de l'Agència Espanyola de Protecció de Dades sobre la k-anonimat com a mesura de la privacitat. Consulta [aquest enllaç](#).
- 10 Malentesos relacionats amb l'anonimització. Consulta [aquest enllaç](#).
- Introducció a l'hash com a tècnica de seudonimització de dades personals. Consulta [aquest enllaç](#).
- Dictamen 05/2014 sobre tècniques d'anonimització. Consulta [aquest enllaç](#).

NOTÍCIES

- **L'AEPD imposa sanció de prevenció per infracció de l'article 13 RGPD relatiu al deure d'informar els interessats sobre el tractament de les seues dades personals. La reclamació es va formular en relació amb el protocol per la Conselleria per a la realització de PCR a l'alumnat, que s'emporten per empreses externes contractades per aquella entitat. Sol·licita que s'elimine la informació i es corregisca el protocol "de manera que cap laboratori puga creuar l'ADN amb dades del propietari sense un consentiment exprés i informat". La Conselleria al·lega que la conservació de les mostres es realitza en condicions d'anonimització. No obstant això, l'AEPD considera que quan les dades personals es recaptin directament de l'interessat, la informació haurà de facilitar-se en el moment mateix en què té lloc aqueixa recollida de dades. Consulta la resolució en [aquest enllaç](#).**
- **L'AEPD imposa una multa de 5.000€ per una infracció de l'article 5.1.c) "minimització de dades". S'interposa una reclamació davant l'AEPD principalment per la publicació d'escrius en internet amb el seu contingut íntegre, figurant en la majoria d'ells els noms i cognoms dels reclamants. Concretament, el número del DNI d'un reclamant, com a part de la signatura digital, sense anonimitzar. En els fonaments de dret, l'AEPD estableix: "Respecte del DNI, corresponga aquest a una persona de caràcter públic o una persona de caràcter privat, o professional, s'entén que el coneixement d'aquesta dada no és rellevant a l'efecte de la finalitat del tractament de B.B.B., atés que sense el mateix es compleix la finalitat d'aquest. En aquest cas, s'imposa l'anonimització d'aquesta dada. La signatura d'un document com el que és objecte de difusió, un escrit privat de reclamant no precisa d'associar el DNI/NIF del seu titular per mes que quin associat o inclòs en la signatura electrònica d'aquest, ja que suficient és la informació i identificació pel nom i cognoms que en molts altres escrits ja figuren d'aquest". Consulta la resolució en [aquest enllaç](#).**