PÍNDOLA 21.- HASH COM A TÈCNICA DE SEUDONIMITZACIÓ DE DADES PERSONALS

L'AEPD1 ha publicat un document destinat a la introducció del Hash com a tècnica de seudonimització de dades personals.

L'estudi està dirigit als responsables de tractaments que vulguin utilitzar implementacions basades en l'ús de funcions hash per a seudonimitzar o anonimitzar dades personals. Es presenten de manera breu els fonaments de les funcions hash, les seves propietats, les possibilitats de reidentificar el missatge que va generar el hash i s'estableixen certes guies per a analitzar l'adequació d'un tractament que utilitzi funcions hash.

Una funció resum o funció hash és un procés que transforma qualsevol conjunt arbitrari de dades en una nova sèrie de caràcters amb una longitud fixa, independentment de la grandària de les dades d'entrada.

El resultat obtingut es denomina hash, resum, digest o imatge. Moltes vegades, el terme "hash" s'utilitza tant per a referir-se a la funció hash com al valor resultat obtingut d'executar aquesta funció sobre un missatge en particular. A les dades que seran processades per la funció hash se'l denomina missatge o preimatge. El conjunt de tots els possibles missatges o preimatge és el domini o espai de missatges.

La utilització de les tècniques de hash per a seudonimitzar o anonimitzar la informació de caràcter personal ha d'estar acompanyada d'una anàlisi dels riscos de reidentificació que té la tècnica de hash concreta empleada en el tractament. En aquesta anàlisi de riscos s'ha d'analitzar tant el procés de hash, com els restants elements que conformen el sistema de hash, amb particular especial atenció a la informació vinculada o vinculable al propi valor representat pel hash. L'anàlisi ha de resultar en una avaluació objectiva de la probabilitat de reidentificació a llarg termini.

Independentment de l'anàlisi de riscos, els elements bàsics a tenir en compte per a la utilització de funcions hash per a la protecció de la informació són, entre altres:

- Alta entropia de la informació a realitzar el hash.
- Utilització de valors de aleatoris d'un sol ús.
- Si escau, grandària d'un valor que surt per sobre de la grandària de bloc del hash, sense ser múltiple de la grandària de bloc.
- Utilitzar generadors d'informació aleatòria apropiats per a tècniques criptogràfiques.
- Accés segur al procés d'execució del hash.
- Nul·la vinculació amb identificadors, seudoidentificadores o una altra informació, en particular en el mateix registre i entre registres o taules/cadenes paral·leles.
- Realitzar auditories periòdiques dels processos de gestió del sistema de hash anonimitzades.

[1] Agència Espanyola de Protecció de Dades

- Quasi-identificadors: són aquells que aïlladament no identifiquen una persona, però agrupats amb altres poden arribar a identificar-la. Amb les tècniques d'anonimització s'han d'eliminar aquest tipus de dades que no siguin necessaris per al tractament.
- Atributs sensibles: són les dades que tenen un major impacte per a la privacitat de la persona com les dades especialment protegides (dades de salut, bancaris, etc.). Aquesta informació pot ser important per al tractament, però es mantindrà dissociada de la persona concreta, llevat que hi hagi legitimació per associar.

Per a considerar la tècnica de hash com a una tècnica d'anonimització, aquesta anàlisi de riscos ha d'avaluar, a més:

- Les mesures organitzatives que garanteixen una eliminació de la informació que permeti la reidentificació.
- Una garantia raonable que el sistema serà robust més enllà de la vida esperada de les dades de caràcter personal.

En definitiva, l'adopció de garanties per a l'aplicació dels principis establerts en el RGPD requereix d'una anàlisi qualitativa rigorosa prèvia per a determinar la seva adequació de manera objectiva.

Per a més informació:

- Introducción al hash como técnica de seudonimización de datos personales https://www.aepd.es/media/estudios/estudio-hash-anonimidad.pdf
- Nota tècnica K-Anonimitat: https://www.aepd.es/media/notas-tecnicas/nota-tecnica-kanonimidad.pdf
- Orientaciones y garantías en los procesos de anonimización https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

-Per qualsevol dubte o aclariment addicional podeu adreçar-vos al DPD de Salut- dpd@ticsalutsocial.cat

https://ticsalutsocial.cat/oficina-dpd/

Tel.: 93 553 26 42 (9:00 a 14:00 h.)