telecos.cat
enginyers de telecomunicació, electrònica i multimèdia-audiovisual

Seinb@
Audit & Consulting

ISACA
Trust in, and value from, information systems
Barcelona Chapter

El nou Reglament Europeu de Protecció de Dades

Obligacions derivades del nou reglament que hauran d'aplicar les enginyeries com a proveïdors de serveis TIC.

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

- El responsable del tractament, triarà únicament un encarregat que ofereixi garanties suficients per aplicar mesures tècniques i organitzatives apropiades, de forma que el tractament estigui d'acord amb el que disposa el RGPD i garanteixi la protecció dels drets dels l'interessats.
- L'encarregat posarà a disposició del responsable tota la informació necessària per demostrar el compliment de les obligacions establertes en el RGPD i en el contracte d'encarregat del tractament, així com permetrà i contribuirà a la realització d'auditories, incloses inspeccions, per part del responsable o d'un altre auditor autoritzat pel responsable.

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Responsabilitat proactiva

- Aplicar mesures tècniques i organitzatives apropiades a fi de garantir i poder demostrar que el tractament és conforme amb el RGPD. Cal analitzar quines dades es tracten, amb quines finalitats i quin tipus d'operacions de tractament es duen a terme. Cal determinar de forma explícita la forma en què aplicaran les mesures que el RGPD preveu, assegurant-se que aquestes mesures són les adequades per complir amb el mateix i que poden demostrar-se davant els interessats i davant les autoritats de control. Aquest principi exigeix una actitud conscient, diligent i proactiva per part de les organitzacions enfront de tots els tractaments de dades personals que duguin a terme.

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Enfoc basat en el risc

- Les mesures dirigides a garantir el compliment del RGPD han de tenir en compte la naturalesa, l'àmbit, el context i les finalitats del tractament així com el risc per als drets i llibertats de les persones. Algunes de les mesures que el RGPD estableix s'aplicaran només quan existeixi un alt risc per als drets i llibertats, mentre que unes altres hauran de modular-se en funció del nivell i tipus de risc que els tractaments presentin. L'aplicació de les mesures previstes ha d'adaptar-se a les característiques de les organitzacions.

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Principis de tractament

- Licitud, lleialtat i transparència. Limitació de la finalitat. Minimització de dades. Exactitud. Limitació del termini de conservació. Integritat i confidencialitat. Responsabilitat proactiva.

Legitimació per al tractament de dades

- Cal incloure la base legal sobre la qual es desenvolupa el tractament en proporcionar la informació quan es recullen les dades dels interessats. També cal especificar i documentar els interessos legítims en què es fonamenten els tractament. (Consentiment, relació contractual, interessos vitals de l'interessat o d'altres persones, obligació legal per al responsable...).

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Consentiment

- El consentiment ha de ser "inequívoc". És aquell que s'ha prestat mitjançant una manifestació de l'interessat o mitjançant una clara acció afirmativa. No s'admeten formes de consentiment tàcit o per omissió, ja que es basen en la inacció.
- Es contemplen situacions en les quals el consentiment, a més d'inequívoc, ha de ser explícit:
  - Tractament de dades sensibles.
  - Adopció de decisions automatitzades.
  - Transferències internacionals.

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Drets dels interessats

- Informació. Accés. Rectificació. Supressió (dret a l'oblit). Limitació del tractament. Portabilitat de les dades. Oposició. Decisions individuals automatitzades, inclosa l'elaboració de perfils.
- L'exercici dels drets serà gratuït per a l'interessat, excepte en els casos en què es formulin sol·licituds manifestament infundades o excessives, especialment si són repetitives.
- S'haurà d'informar a l'interessat sobre les actuacions derivades de la seva petició en el termini d'un mes, excepte en casos complexos, en que el termini serà de dos mesos.

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Relacions Responsable - Encarregat

- Els encarregats tenen obligacions pròpies que estableix el RGPD, que són implícites independentment de l'àmbit del contracte amb ell responsable. Entre altres, han de mantenir un registre d'activitats de tractament, han de determinar les mesures de seguretat aplicables als tractaments que realitzen, ...
- El responsable haurà d'adoptar mesures apropiades, inclosa l'elecció d'encarregats, de manera que garanteixi i estigui en condicions de demostrar que el tractament es realitza conforme el RGPD.
- Per demostrar que els encarregats ofereixen les garanties exigides pel RGPD, aquests poden adherir-se a codis de conducta o certificar-se tal i com especifica el RGPD.

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Relacions Responsable - Encarregat

- Les relacions entre el responsable i l'encarregat han de formalitzar-se en un contracte o acte jurídic que els vinculi. El contingut mínim dels contractes per encàrrec, havent de preveure entre altres, aspectes com:
  - Objecte, durada, naturalesa i la finalitat del tractaments.
  - Tipus de dades personals i categories d'interessats.
  - Tractar les dades personals únicament seguint instruccions documentades del responsable
  - El responsable ha de donar la seva autorització prèvia a les subcontractacions
  - Assistència al responsable, sempre que sigui possible, en l'atenció a l'exercici de drets dels interessats...

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Anàlisi del risc

- Tots els responsables hauran de realitzar una valoració del risc dels tractaments que realitzin, a fi de poder establir què mesures han d'aplicar i com han de fer-ho.
- Com a regla general, l'anàlisi haurà de dur-se a terme utilitzant alguna de les metodologies d'anàlisis de risc existents. En organitzacions petites i molt petites, i amb tractaments de poca complexitat: l'anàlisi serà el resultat d'una reflexió, mínimament documentada, sobre les implicacions dels tractaments en els drets i llibertats dels interessats

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Registre d'activitats de tractament

- S'haurà de mantenir un registre d'activitats de tractament en el qual es contingui la informació que estableix el RGPD.
- Encara que, estan exemptes les organitzacions de menys de 250 empleats, tret que el tractament que realitzin pugui comportar un risc per als drets i llibertats dels interessats, no sigui ocasional o inclogui categories especials de dades o dades relatives a condemnes i infraccions penals, es recomanable mantenir-lo com a guia dels tractaments que es duen a terme.

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Protecció de dades des del disseny

- La protecció de dades des del disseny suposa aplicar les garanties necessàries de protecció des de la fase inicial de planificació per a qualsevol producte o servei.
- En el fons és una precaució que proporcionarà un estalvi de recursos, ja que és més fàcil planificar i desenvolupar des de l'inici sobre la base d'un adequat marc legal que no desenvolupar-ho a posteriori.
- És una mesura proactiva que busca la protecció en tot el cicle de vida del producte o servei.

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Protecció de dades per defecte

- La protecció de dades per defecte consisteix a oferir les màximes garanties de privacitat per defecte en productes o serveis que vagin a tractar dades personals, és a dir, si hi ha diverses configuracions de privacitat, hauran de venir marcades per defecte aquelles que ofereixin majors garanties de privacitat a l'interessat.

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Mesures de seguretat

- Els responsables i encarregats establiran les mesures tècniques i organitzatives apropiades per garantir un nivell de seguretat adequat en funció dels riscos detectats en l'anàlisi de riscos.
- Les mesures tècniques i organitzatives hauran d'establir-se tenint en compte els riscos per als drets i llibertats de les persones, la naturalesa, l'abast, el context i les finalitats del tractament, el cost de la tècnica i els costos d'aplicació.

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Notificació de violacions de seguretat de les dades

- Les violacions de seguretat de les dades és tot incident que ocasioni la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra forma, o la comunicació o accés no autoritzats a aquestes dades.
- Quan es produeixi una violació de la seguretat de les dades, el responsable ha de notificar-la a l'autoritat de protecció de dades competent, tret que sigui improbable que la violació suposi un risc per als drets i llibertats dels afectats.
- La notificació de la fallida a les autoritats ha de produir-se sense dilació indeguda i, si pot ser, dins de les 72 hores següents al fet que el responsable tingui constància d'ella.

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Avaluació d'Impacte sobre la Protecció de Dades

- Els responsables de tractament hauran de realitzar una Avaluació d'Impacte sobre la Protecció de Dades amb caràcter previ a la posta en marxa d'aquells tractaments que sigui probable que comportin un alt risc per als drets i llibertats dels interessats.

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Delegat de Protecció de Dades

- El Delegat de Protecció de Dades , és obligatori en les autoritats i organismes públics, responsables o encarregats que tinguin entre les seves activitats principals les operacions de tractament que requereixin una observació habitual i sistemàtica d'interessats a gran escala, responsables o encarregats que tinguin entre les seves activitats principals el tractament a gran escala de dades sensibles.

OBLIGACIONS DE COMPLIMENT COM A PROVEÏDORS DE SERVEIS TIC

Transferències internacionals

- El model de transferències internacionals dissenyat pel RGPD segueix els mateixos criteris que l'establert per la Directiva 95/46 i per les legislacions nacionals de transposició.
- S'amplia la llista de possibles instruments per oferir garanties, incloent-se expressament, entre altres, les Normes Corporatives Vinculants per a responsables i encarregats, els codis de conducta i esquemes de certificació, així com els clàusules contractuals tipus que puguin aprovar les autoritats de protecció de dades.

MOLTES GRÀCIES!!!

Francesc Flores

Seinba Audit & Consulting

francesc.flores@seinba.com