UNITAT DE CONEIXEMENT

Novembre 2018

Adaptació a la nova Llei de Protecció de Dades

"La tecnologia permet que tant les empreses privades com les autoritats públiques utilitzin dades personals a una escala sense precedents"

Preàmbul a l'RGPD

fundació factor humà

Què és?

- ✓ El **Reglament General de Protecció de Dades** (RGPD) és un reglament europeu que va entrar en vigor el 25 de maig de 2018 amb l'objectiu d'enfortir i unificar la protecció de dades personals a tots els països de la Unió europea (UE), controlant també la transferència de dades fora de la Unió tot unificant el marc regulador per a les multinacionals. És una normativa **més estricta** que les anteriors i suposa la primera norma sobre aquesta matèria que afecta tots els països de la UE i n'unifica tant els drets com les obligacions.
    - ❖ Els **dos aspectes que han fet visible** per a la ciutadania l'entrada en vigor de la nova normativa han estat la recepció durant el mes de maig de nombrosos correus electrònics en els quals se'ls sol·licitava la revalidació de la cessió de dades a efectes de rebre informacions periòdiques, així com l'aparició de notificacions per a autorització d'ús de *cookies* a la pràctica totalitat de pàgines web.
- ✓ L'**adaptació a la nova legislació** suposa tot un repte per a les organitzacions i els Departaments de Recursos Humans. El *World Economic Forum* ja considera des de 2011 les dades personals com **un nou tipus d'actiu** que cal gestionar i regular. A les dades tradicionals com el nom, telèfon, direcció postal o dades financeres, cal afegir-hi les **noves mètriques** que generen els canvis tecnològics i socials com ara els hàbits de navegació o les dades biomètriques i genètiques.
- ✓ Les principals **novetats** de la nova regulació són:
    - **Consentiment reforçat**: la persona usuària o client haurà de donar el seu consentiment **específic**, **inequívoc i circumscrit** a cada ús **concret**. No s'admeten consentiments genèrics, tàcits o ambigus.
    - **Limitació temporal**: ha d'explicitar-se en el tractament de la informació i és un dret que se suma als ja existents d'accés, rectificació, cancel·lació i oposició.
    - **Dret a l'oblit**: facilitar que s'eliminin informacions que danyin la reputació d'una persona a perpetuïtat (amb la limitació d'informacions d'interès públic).
    - **Portabilitat de les dades**: dret a descarregar-se la informació que s'ha cedit a un servei o organització i moure-la a un altre servei o plataforma.

- **Cobertura global**: afecta també aquelles organitzacions situades fora de la UE que realitzen activitats dins de la Unió que impliquin el tractament de dades personals, fins i tot encara que no tinguin presència física en el territori de la Unió.
- **Minimització**: en el disseny de software i de processos, la normativa requereix una **privacitat per defecte**, és a dir, l'ús de la mínima quantitat de dades personals imprescindibles per a la finalitat per a la qual s'ha rebut autorització.
- **Dimensió sancionadora**: la normativa preveu multes de fins a 20 milions d'euros o el 4% del volum de facturació de l'organització en casos d'incompliments greus.

Eines

✓ **Processos de selecció**: durant aquests processos es gestionen una gran quantitat de dades personals. Cal incorporar i acreditar els principis recollits a la nova regulació:

- Transparència, qualitat de les dades, minimització i **terminis de conservació de dades limitats en el temps** (aquells currículums que no hagin estat actualitzats no poden conservar-se més enllà de **24 mesos** i han de ser esborrats).
- És imprescindible el **consentiment explícit** a la recollida de dades, així com que les persones candidates manifestin si volen ser contactades de nou en **futurs processos** de selecció i/o per a **altres posicions** vacants.
- En el cas que iniciem el contacte amb la persona candidata, nosaltres (sempre mitjançant un correu o plataforma on hagi publicat obertament les dades de contacte), caldrà que l'informem en el **primer correu** de la nostra política de protecció de dades i demanem el seu consentiment per a futures comunicacions.
- Totes les persones candidates tenen dret a consultar quines dades hem reunit d'elles o demanar una **portabilitat** d'aquestes dades.
- És evident que la **digitalització** dels processos de selecció resulta gairebé indispensable per gestionar aquests requisits legals i garantir la privacitat de les dades durant tot el procés. És molt difícil establir l'antiguitat de currículums impresos en paper que van acumulant-se pel despatx.

✓ **Comunicació de dades a tercers**: si una organització externa ens gestiona la totalitat o part d'algun procés, caldrà ser extremament

vigilants en l'acompliment de la normativa i documentar tot el procés de cessió de dades. Alguns dels processos de RH més habituals en què solen intervenir tercers són formació, gestió de nòmines o assistència en l'expatriació.

- En totes aquestes comunicacions ha de regir el principi de **minimització**, és a dir, comunicar les mínimes dades necessàries per al procés encomanat a tercers (i sempre amb autorització de les persones).
- Caldrà vetllar per l'acompliment fins i tot si la comunicació es produeix entre organitzacions del mateix grup.

✓ **Formació específica en protecció de dades**: no només enfocat a les persones que directament gestionin processos amb molt volum de dades, sinó que també és recomanable formar les persones per tal que canviïn vells hàbits que poden suposar un risc de seguretat (consulta 'L'experiència' de *Barcroft Media* per a recomanacions sobre la gestió dels escriptoris).

✓ ***Big Data***: l'RGPD en certa manera ha "refredat" les expectatives que en els darrers anys s'havien dipositat en la *big data* com a eina de gestió dels RH. Planteja moltes ombres legals i ètiques l'encreuament de dades recollides en diferents processos de diversa finalitat per a la formulació de prediccions amb altres objectius que no compten amb autorització explícita. Aquest refredament ha vingut de la mà d'un canvi social en la percepció dels efectes de la *big data*. Segons una enquesta de *Gartner*, el 75% de les persones enquestades pensen que la Intel·ligència Artificial destruirà la seva privacitat en lloc de millorar-la.

✓ **Persona responsable/encarregada del tractament de dades**:

- El/La **responsable** del fitxer o **registre de les activitats de tractament de dades** és la persona física o jurídica que decideix sobre el tractament de les dades, què se'n farà, si es conservaran, se cediran o s'eliminaran.
- L'**encarregat/da** és la persona física o jurídica que tracta dades personals per encàrrec del/de la responsable del tractament. Sol ser un tercer extern a l'empresa. És el cas, per exemple, d'assessories laborals, mútues de prevenció de riscos, etc. L'RGPD regula **obligacions pròpies** dels encarregats. Per demostrar que aquests encarregats ofereixen les garanties exigides per l'RGPD podran adherir-se a codis de conducta o certificar-se dins dels esquemes previstos per l'RGPD, a banda de mantenir el seu propi registre d'activitats. També cal incorporar les previsions del RGPD als **contractes** de cessió de dades. L'*AEPD* ha publicat unes directrius per a la redacció d'aquest tipus de contractes (consulta la secció de 'Materials en línia')

✓ **Delegat/da de protecció de dades**: és una figura que l'RGPD estableix com a obligatòria en el cas d'administracions públiques o d'organitzacions

l'activitat principal de les quals impliquin el tractament de dades personals. Les seves funcions són:

- Informar i assessorar les persones responsables i encarregades del tractament de dades personals (i als seus empleats i empleades) sobre les obligacions.
- Supervisar el compliment de la legislació i de la política de protecció de dades.
- Cooperar amb les autoritats (Agències de Protecció de Dades) com a "punt de contacte".

La dada

Segons un estudi de l'organització d'integració de dades al núvol *Talend* amb una mostra de 103 organitzacions que operen a Europa, quatre mesos després de l'entrada en vigor del RGPD el 70% de les organitzacions incompleixen la nova regulació perquè no tenen mecanismes per facilitar una còpia de les dades personals de les persones usuàries que així ho demanin. El grau de compliment més alt es produeix al sector financer, mentre que les petites i mitjanes empreses i el sector *retail* registren compliments molt minoritaris.

Guia de Treball

ESTEM COMPLINT L'RGPD?

- **Algunes de les preguntes que ens podem formular per situar el nostre grau de compliment són:**
  - **Estem obligats a tenir un Registre de les activitats de tractament i un/a Delegat/da de protecció de dades?**
  - **Hem avaluat els proveïdors amb accés a dades (assessoria fiscal, comptable i/o laboral, empreses d'informàtica, agències de màrqueting, etc.) i els hem fet signar el nou contracte d'encarregat de tractament?**
  - **Hem actualitzat les clàusules informatives en formularis en paper, pàgina web, xarxes socials, etc.?**
  - **Hem verificat que tenim el consentiment de les persones usuàries i/o clients per al tractament de les seves dades? Podem demostrar aquest consentiment?**
  - **Hem digitalitzat els processos que comporten un tractament de dades personals per a un millor seguiment dels requisits legals?**

MESURES D'AVALUACIÓ I DISSENY

- **Els/Les responsables de tractament hauran de realitzar una Avaluació d'Impacte sobre la Protecció de Dades (AIPD) amb caràcter previ a la posada en funcionament d'aquells tractaments que molt probablement comportin un alt risc per a la privacitat de les persones interessades. Alguns exemples són:**
  - **Elaboració de perfils sobre la base dels quals es prenguin decisions que produeixin efectes jurídics.**
  - **Tractaments a gran escala de dades sensibles.**
  - **Observació sistemàtica a gran escala d'una zona d'accés públic.**
- **Un altre exemple d'aquesta actitud proactiva que exigeix l'RGPD és la necessitat de la protecció de dades per disseny i per defecte. Des de l'inici, i amb anterioritat al tractament de dades, els/les responsables han d'adoptar mesures que garanteixin que només es tractaran les dades necessàries pel que fa a la quantitat, abast temporal del tractament, períodes de conservació i accessibilitat de les dades. Això inclou una anàlisi prèvia de risc.**

MESURES DE RESPONSABILITAT ACTIVA

- ***Manteniment del Registre de les activitats de tractament*** **(exemptes les organitzacions de menys de 250 treballadors/es). Ha de contenir: nom i dades de contacte de la persona responsable i de la Delegada de protecció de dades (si existeix), finalitats del tractament, descripció de categories d'interessats i categories de dades personals tractades, transferències internacionals de dades.**
- ***Mesures de seguretat*****: mesures tècniques i organitzatives apropiades per garantir un nivell de seguretat adequat en funció dels riscos detectats en l'anàlisi prèvia. En alguns casos els/les responsables podran seguir aplicant les mateixes mesures que se seguien amb la legislació anterior (LOPD) si els resultats de l'anàlisi prèvia de riscos conclou que les mesures ofereixen un nivell de seguretat adequat. En altres casos, serà necessari completar-les amb mesures addicionals.**
- ***Notificació de violacions de seguretat de les dades*****: quan es produeixi una violació de la seguretat de les dades, la persona 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 de les persones afectades. La notificació a les autoritats ha de produir-se sense dilació indeguda i, si pot ser, dins de les 72 hores següents.**

Consulta 'Materials en línia' per veure la *Guia del RGPD per a responsables*

L'experiència

- *Facebook* és una coneguda xarxa social amb més de 2.000 milions de persones usuàries actives al mes. Ha diversificat el seu negoci amb l'adquisició de 71 organitzacions, entre elles el popular servei de missatgeria *WhatsApp* o el fabricant d'interfícies de realitat virtual *Oculus VR*. És la cinquena organització amb més pes a l'índex borsari NASDAQ per darrere d'*Apple*, *Microsoft*, *Amazon* i *Google*.
- Tot i que més del 60% del seu volum de negoci el genera als EUA i Canada, Europa suposa per a *Facebook* uns ingressos de més de 3.000 milions de dòlars per quadrimestre, la pràctica totalitat provinent de la publicitat. La seva operativa basada en la recopilació i l'encreuament de dades personals i de navegació s'ha vist especialment afectada per les noves i més estrictes regulacions de privadesa europees.
- Aquesta **divergència entre els marcs regulatoris** del seu país d'origen i l'europeu planteja seriosos esculls en l'operativa d'organitzacions globals i transfrontereres i no només en el cas de *Facebook*. Més de quaranta diaris nord-americans, entre ells el *LA Times* i el *Chicago Tribune*, van deixar de ser accessibles a Europa arran de l'entrada en vigor del RGPD per impossibilitat o manca de voluntat d'ajustar-se als nous requisits de privadesa.
- El fundador de *Facebook*, Mark Zuckerberg, va anunciar de manera vaga la intenció de traslladar la majoria de noves proteccions europees als usuaris estatunidencs durant la seva compareixença davant un comitè del Senat nord-americà. Aquesta compareixença fou motivada per un escàndol de filtració de dades personals a tercers (*Cambridge Analytica*). El dubte roman sobre la capacitat de *Facebook* d'adaptar-se a aquests requisits i alhora sostenir una expansió que ha estat basada en l'autoregulació i un ús lax de les dades de les seves persones usuàries.
- La posició dominant de *Facebook* en el sector de les xarxes socials planteja serioses ombres sobre l'ús ètic de la informació recopilada i el seu ús per generar **campanyes d'opinió** durant períodes preelectorals o personalitzar els anuncis segons el nostre perfil d'interessos.

BARCROFT MEDIA

- ✓ *Barcroft Media* és una productora audiovisual per a mitjans de comunicació i canals *online* especialitzada a oferir contingut que resulti atractiu a ulls de la generació de nadius digitals (imatges, vídeos i reportatges). Compta amb una gran presència a *Youtube*, on s'ha convertit en el cinquè proveïdor de notícies amb més de cinc milions i mig de subscriptors. Té oficines a Londres, Nova York i Delhi.
- ✓ *Barcroft Media* ha parat esment en un aspecte de la nova regulació de protecció de dades que se sol ignorar: la regulació no només afecta les dades que tinguem en formats digitals, sinó també en **suports físics**. Per això, han identificat els **escriptoris desordenats** i la paperassa esfullada sobre les taules com un potencial risc de filtracions de dades personals.
- ✓ Per evitar-ho han establert una estricta normativa interna: les seves 50 persones empleades ja no poden deixar la **paperassa damunt la taula**. Els documents, inclosos els quaderns de notes, targetes de visita i els papers amb anotacions, es guarden tancats en calaixos durant la nit.
- ✓ Segons Dave Wheels, cap d'Operacions de l'organització, aquesta tolerància zero davant els escriptoris desordenats consciencia les persones treballadores que **alguna cosa ha canviat** de manera indiscutible amb la nova legislació. Aquesta política s'alinea amb les **recomanacions** per a la minimització de riscos de privacitat als escriptoris de treball:
  - No deixar contrasenyes escrites en *post-its* o altres llocs accessibles.
  - Bloquejar tots els dispositius de la feina amb contrasenyes.
  - Netejar la taula de treball al final del dia i arxivar amb clau els documents sensibles.
  - No imprimir un document si no és necessari i destruir-lo després de fer-ne ús si no considerem que hagi de ser arxivat.
  - Usar calaixos i arxivadors que tanquin amb clau.
  - Formar la plantilla en riscos per a la privacitat.

Materials

Bibliografia bàsica

Blázquez Agudo, Eva Mª. *Aplicación práctica de la protección de datos en las relaciones laborales*. CISS, 2018.

Preciado Domènech, Carlos Hugo. *El derecho a la protección de datos en el contrato de trabajo*. Aranzadi, 2017.

Materials en línia

Itziar de Lecuona i Genís Roca expliquen el nou RGPD (vídeo)

Entrevista de Xavier Grasset al programa *Més 324* de *Televisió de Catalunya* a Genís Roca, president de RocaSalvatella, i a Itziar de Lecuona, professora i sotsdirectora de l'Observatori de Bioètica i Dret de la Universitat de Barcelona.

http://www.ccma.cat/tv3/alacarta/mes-324/itziar-de-lecuona-i-genis-roca-expliquen-el-nou-reglament-de-proteccio-de-dades-rgpd/video/5767915/

Adaptación al RGPD en el sector privado (pdf)

Full de ruta sintètic amb 6 passes per a l'adaptació del RGPD a la nostra organització.

https://www.aepd.es/media/infografias/infografia-adaptacion-rgpd-sector-privado.pdf

Guía del RGPD para responsables de tratamiento (pdf)

Completa publicació conjunta de diverses agències de protecció de dades (estatal, catalana i basca) per a ús de responsables del tractament. A més de la descripció dels requisits legals, inclou recomanacions en cadascun dels apartats.

https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

Reglament general de protecció de dades

Portal de la *Generalitat de Catalunya* que ofereix preguntes freqüents i guies (entre elles, una pensada per a persones encarregades) sobre el compliment del reglament. Inclou una traducció (no oficial) del reglament al català, a més de les versions castellana i anglesa.

http://apdcat.gencat.cat/ca/documentacio/RGPD/

Directrices para elaborar contratos entre responsables y encargados del tratamiento (pdf)

Guia que delimita les funcions i responsabilitats de responsables i encarregats, i ofereix pautes per a una correcta elaboració i seguiment dels contractes.

https://www.aepd.es/media/guias/guia-directrices-contratos.pdf

Gugel, José Luis. "El RGPD, la captación del talento y la digitalización". *Expansión*, 12/09/2018.

Article que aclareix com l'RGPD no impedeix la captació activa de talent, però si regula com ha d'establir-se la comunicació i les autoritzacions explícites que calen per prosseguir-la.

http://www.expansion.com/juridico/opinion/2018/09/12/5b99424546163f7e888b45a0.html

Facchin, José. "¿Cómo adaptar tu negocio al nuevo RGPD europeo 2018?". *El Blog de José Facchin*, 06/05/2018.

Article amb un enfocament pràctic i diferents supòsits d'aplicació. Inclou una comparació entre els antics requisits de la LOPD i les noves obligacions generades per l'RGPD.

https://josefacchin.com/rgpd/

Mendieta, Carles. "Els límits de la Intel·ligència Artificial: una mirada optimista amb tocs d'alerta". *Blog Factor Humà*, 12/09/2018.

Debat sobre els límits de la Intel·ligència Artificial entre Genis Roca, president de *Roca Salvatella*, i Itziar de Lecuona, sotsdirectora de l'*Observatori de Bioètica i Dret de la UB* en el marc de l'acte de lliurament dels *Premis Factor Humà*.

https://factorhuma.org/ca/actualitat/blog-factor-huma/13704-els-limits-de-la-intel-ligencia-artificial-una-mirada-optimista-amb-tocs-d-alerta