UNIDAD DE CONOCIMIENTO

Noviembre 2018

Adaptación a la nueva Ley de Protección de Datos

"La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales a una escala sin precedentes"

Preámbulo a la RGPD

fundació factor humà

¿Qué es?

- El **Reglamento General de Protección de Datos** (RGPD) es un reglamento europeo que entró en vigor el 25 de mayo de 2018 con el objetivo de fortalecer y unificar la protección de datos personales en todos los países de la Unión Europea (UE), controlando también la transferencia de datos fuera de la Unión unificando el marco regulador para las multinacionales. Es una normativa **más estricta** que las anteriores y supone la primera norma sobre esta materia que afecta a todos los países de la UE y unifica tanto los derechos como las obligaciones.
    - Los **dos aspectos que han hecho visible** para la ciudadanía la entrada en vigor de la nueva normativa han sido la recepción durante el mes de mayo de numerosos correos electrónicos en los cuales se les solicitaba la revalidación de la cesión de datos a efectos de recibir informaciones periódicas, así como la aparición de notificaciones para autorización de uso de *cookies* en la práctica totalidad de páginas web.
- La **adaptación a la nueva legislación** supone todo un reto para las organizaciones y los Departamentos de Recursos Humanos. El *World Economic Forum* ya considera desde 2011 los datos personales como **un nuevo tipo de activo** que hay que gestionar y regular. A los datos tradicionales como el nombre, teléfono, dirección postal o datos financieros, hay que añadir las **nuevas métricas** que generan los cambios tecnológicos y sociales como, por ejemplo, los hábitos de navegación o los datos biométricos y genéticos.
- Las principales **novedades** de la nueva regulación son:
    - **Consentimiento reforzado**: la persona usuaria o cliente tendrá que dar su consentimiento **específico**, **inequívoco y circunscrito** a cada uso **concreto**. No se admiten consentimientos genéricos, tácitos o ambiguos.
    - **Limitación temporal**: tiene que explicitarse en el tratamiento de la información y es un derecho que se suma a los ya existentes de acceso, rectificación, cancelación y oposición.
    - **Derecho al olvido**: facilitar que se eliminen informaciones que dañen la reputación de una persona a perpetuidad (con la limitación de informaciones de interés público).
    - **Portabilidad de los datos**: derecho a descargarse la información que se ha cedido a un servicio u organización y moverla a otro servicio o plataforma.

- **Cobertura global**: afecta también a aquellas organizaciones situadas fuera de la UE que realicen actividades dentro de la Unión que impliquen el tratamiento de datos personales, incluso aunque no tengan presencia física en el territorio de la Unión.
- **Minimización**: en el diseño de software y de procesos, la normativa requiere una **privacidad por defecto**, es decir, el uso de la mínima cantidad de datos personales imprescindibles para la finalidad para la que se ha recibido autorización.
- **Dimensión sancionadora**: la normativa prevé multas de hasta 20 millones de euros o el 4% del volumen de facturación de la organización en casos de incumplimientos graves.

Herramientas

✓ **Procesos de selección**: durante estos procesos se gestionan una gran cantidad de datos personales. Hay que incorporar y acreditar los principios recogidos en la nueva regulación:

- Transparencia, calidad de los datos, minimización y **plazos de conservación de datos limitados en el tiempo** (aquellos currículums que no hayan sido actualizados no pueden conservarse más allá de **24 meses** y tienen que ser eliminados).
- Es imprescindible el **consentimiento explícito** en la recopilación de datos, así como que las personas candidatas manifiesten si quieren ser contactadas de nuevo en **futuros procesos** de selección y/o para **otras posiciones** vacantes.
- En el caso de que iniciemos el contacto con la persona candidata, nosotros (siempre mediante un correo o plataforma donde haya publicado abiertamente los datos de contacto), hará falta que le informemos en el **primer correo** de nuestra política de protección de datos y pidamos su consentimiento para futuras comunicaciones.
- Todas las personas candidatas tienen derecho a consultar qué datos hemos reunido de ellas o pedir una **portabilidad** de dichos datos.
- Es evidente que la **digitalización** de los procesos de selección resulta casi indispensable para gestionar estos requisitos legales y garantizar la privacidad de los datos durante todo el proceso. Es muy difícil establecer la antigüedad de currículums impresos en papel que van acumulándose por el despacho.

✓ **Comunicación de datos a terceros**: si una organización externa nos gestiona la totalidad o parte de algún proceso, se deberá ser

extremamente vigilantes en el desempeño de la normativa y documentar todo el proceso de cesión de datos. Algunos de los procesos de RH más habituales en que suelen intervenir terceros son formación, gestión de nóminas o asistencia en la expatriación.

- En todas estas comunicaciones tiene que regir el principio de **minimización**, es decir, comunicar los mínimos datos necesarios para el proceso encomendado a terceros (y siempre con autorización de las personas).
- Se deberá velar por el desempeño incluso si la comunicación se produce entre organizaciones del mismo grupo.

✓ **Formación específica en protección de datos**: no solo enfocado a las personas que directamente gestionen procesos con mucho volumen de datos, sino que también es recomendable formar a las personas para que cambien viejos hábitos que puedan suponer un riesgo de seguridad (consulta 'La experiencia' de *Barcroft Media* para recomendaciones sobre la gestión de los escritorios).

✓ ***Big Data***: la RGPD en cierto modo ha "enfriado" las expectativas que en los últimos años se habían depositado en el *big data* como herramienta de gestión de los RH. Plantea muchas sombras legales y éticas el cruce de datos recogidos en los diferentes procesos de diversa finalidad para la formulación de predicciones con otros objetivos que no cuentan con autorización explícita. Este enfriamiento ha venido de la mano de un cambio social en la percepción de los efectos del *big data*. Según una encuesta de *Gartner*, el 75% de las personas encuestadas piensan que la Inteligencia Artificial destruirá su privacidad en lugar de mejorarla.

✓ **Persona responsable/encargada del tratamiento de datos**:

- El/La **responsable** del fichero o **registro de las actividades de tratamiento de datos** es la persona física o jurídica que decide sobre el tratamiento de los datos, qué se hará, si se conservarán, se cederán o se eliminarán.
- El **encargado/a** es la persona física o jurídica que trata datos personales por encargo del/de la responsable del tratamiento. Suele ser un tercero externo a la empresa. Es el caso, por ejemplo, de asesorías laborales, mutuas de prevención de riesgos, etc. El RGPD regula **obligaciones propias** de los encargados. Para demostrar que estos encargados ofrecen las garantías exigidas por el RGPD podrán adherirse a códigos de conducta o certificarse dentro de los esquemas previstos por el RGPD, además de mantener su propio registro de actividades. También hay que incorporar les previsiones del RGPD a los **contratos** de cesión de datos. La *AEPD* ha publicado unas directrices para la redacción de este tipo de contratos (consulta la sección de 'Materiales en línea')

✓ **Delegado/a de protección de datos**: es una figura que el RGPD establece como obligatoria en el caso de administraciones públicas o de

organizaciones cuya actividad principal implique el tratamiento de datos personales. Sus funciones son:

- Informar y asesorar a las personas responsables y encargadas del tratamiento de datos personales (y sus empleados y empleadas) sobre las obligaciones.
- Supervisar el cumplimiento de la legislación y de la política de protección de datos.
- Cooperar con las autoridades (Agencias de Protección de Datos) como "punto de contacto".

El dato

Según un estudio de la organización de integración de datos en la nube *Talend* con una muestra de 103 organizaciones que operan en Europa, cuatro meses después de la entrada en vigor del RGPD el 70% de las organizaciones incumplen la nueva regulación porque no tienen mecanismos para facilitar una copia de los datos personales de las personas usuarias que así lo pidan. El grado de cumplimiento más alto se produce en el sector financiero, mientras que las pequeñas y medianas empresas y el sector *retail* registran cumplimientos muy minoritarios.

Guía de Trabajo

¿ESTAMOS CUMPLIENDO EL RGPD?

- **Algunas de las preguntas que nos podemos formular para situar nuestro grado de cumplimiento son:**
  - **¿Estamos obligados a tener un Registro de las actividades de tratamiento y un/a Delegado/a de protección de datos?**
  - **¿Hemos evaluado a los proveedores con acceso a datos (asesoría fiscal, contable y/o laboral, empresas de informática, agencias de marketing, etc.) y les hemos hecho firmar el nuevo contrato de encargo de tratamiento?**
  - **¿Hemos actualizado las cláusulas informativas en formularios en papel, página web, redes sociales, etc.?**
  - **¿Hemos verificado que tenemos el consentimiento de las personas usuarias y/o clientes para el tratamiento de sus datos? ¿Podemos demostrar dicho consentimiento?**
  - **¿Hemos digitalizado los procesos que comportan un tratamiento de datos personales para un mejor seguimiento de los requisitos legales?**

MEDIDAS DE EVALUACIÓN Y DISEÑO

- **Los/Las responsables de tratamiento deberán realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) con carácter previo a la puesta en funcionamiento de aquellos tratamientos que muy probablemente comporten un alto riesgo para la privacidad de las personas interesadas. Algunos ejemplos son:**
  - **Elaboración de perfiles sobre la base de los cuales se tomen decisiones que produzcan efectos jurídicos.**
  - **Tratamientos a gran escala de datos sensibles.**
  - **Observación sistemática a gran escala de una zona de acceso público.**
- **Otro ejemplo de esta actitud proactiva que exige el RGPD es la necesidad de la protección de datos por diseño y por defecto. Desde el inicio, y con anterioridad al tratamiento de datos, los/as responsables tienen que adoptar medidas que garanticen que solo se tratarán los datos necesarios en cuanto a la cantidad, alcance temporal del tratamiento, periodos de conservación y accesibilidad de los datos. Esto incluye un análisis previo de riesgo.**

MEDIDAS DE RESPONSABILIDAD ACTIVA

- ***Mantenimiento del Registro de las actividades de tratamiento*** **(exentas las organizaciones de menos de 250 trabajadores/as). Debe contener: nombre y datos de contacto de la persona responsable y de la Delegada de protección de datos (si existe), finalidades del tratamiento, descripción de categorías de interesados y categorías de datos personales tratados, transferencias internacionales de datos.**
- ***Medidas de seguridad*****: medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo. En algunos casos los/as responsables podrán seguir aplicando las mismas medidas que se seguían con la legislación anterior (LOPD) si los resultados del análisis previo de riesgos concluye que las medidas ofrecen un nivel de seguridad adecuado. En otros casos, será necesario completarlas con medidas adicionales.**
- ***Notificación de violaciones de seguridad de los datos*****: cuando se produzca una violación de la seguridad de los datos, la persona responsable debe notificarla a la autoridad de protección de datos competente, salvo que sea improbable que la violación suponga un riesgo para los derechos y libertades de las personas afectadas. La notificación a las autoridades tiene que producirse sin más dilación indebida, y si puede ser, dentro de las 72 horas siguientes.**

Consulta `Materiales en línea' para ver la *Guía del RGPD para responsables*

La experiencia

- ✓ *Facebook* es una conocida red social con más de 2.000 millones de personas usuarias activas al mes. Ha diversificado su negocio con la adquisición de 71 organizaciones, entre ellas el popular servicio de mensajería *Whatsapp* o el fabricante de *interfaces* de realidad virtual *Oculus VR*. Es la quinta organización con más peso en el índice bursátil NASDAQ por detrás de *Apple*, *Microsoft*, *Amazon* y *Google*.
- ✓ A pesar de que más del 60% de su volumen de negocio lo genera en los EEUU y Canadá, Europa supone para *Facebook* unos ingresos de más de 3.000 millones de dólares por cuatrimestre, la práctica totalidad proveniente de la publicidad. Su operativa basada en la recopilación y el cruce de datos personales y de navegación se ha visto especialmente afectada por las nuevas y más estrictas regulaciones de privacidad europeas.
- ✓ Esta **divergencia entre los marcos regulatorios** de su país de origen y el europeo plantea serios obstáculos en la operativa de organizaciones globales y transfronterizas y no solo en el caso de *Facebook*. Más de cuarenta diarios norteamericanos, entre ellos el *LA Times* y el *Chicago Tribune*, dejaron de ser accesibles en Europa a raíz de la entrada en vigor del RGDP por imposibilidad o carencia de voluntad de ajustarse a los nuevos requisitos de privacidad.
- ✓ El Fundador de *Facebook*, Mark Zuckerberg, anunció de manera vaga la intención de trasladar la mayoría de nuevas protecciones europeas a los usuarios estadounidenses durante su comparecencia ante un comité del Senado norteamericano. Esta comparecencia fue motivada por un escándalo de filtración de datos personales a terceros (*Cambridge Analytica*). La duda permanece sobre la capacidad de *Facebook* de adaptarse a estos requisitos y a la vez sostener una expansión que ha sido basada en la autorregulación y un uso laxo de los datos de sus personas usuarias.
- ✓ La posición dominante de *Facebook* en el sector de les redes sociales plantea serias sombras sobre el uso ético de la información recopilada y su uso para generar **campañas de opinión** durante períodos preelectorales o personalizar los anuncios según nuestro perfil de intereses.

BARCROFT MEDIA

- ✓ *Barcroft Media* es una productora audiovisual para medios de comunicación y canales *online* especializada en ofrecer contenido que resulte atractivo a ojos de la generación de nativos digitales (imágenes, vídeos y reportajes). Cuenta con una gran presencia en *Youtube*, donde se ha convertido en el quinto proveedor de noticias con más de cinco millones y medio de suscriptores. Tiene oficinas en Londres, Nueva York y Delhi.
- ✓ *Barcroft Media* ha prestado atención en un aspecto de la nueva regulación de protección de datos que se suele ignorar: la regulación no solo afecta a los datos que tengamos en formatos digitales, sino también a **soportes físicos**. Por eso, han identificado los escritorios desordenados y el papeleo esparcido sobre las mesas como un potencial riesgo de filtraciones de datos personales.
- ✓ Para evitarlo han establecido una estricta normativa interna: sus 50 personas empleadas ya no pueden dejar el **papeleo sobre la mesa**. Los documentos, incluidos los cuadernos de notas, tarjetas de visita y los papeles con anotaciones, se guardan cerrados en cajones durante la noche.
- ✓ Según Dave Wheels, Jefe de Operaciones de la organización, esta tolerancia cero ante los escritorios desordenados conciencia a las personas trabajadoras que **algo ha cambiado** de manera indiscutible con la nueva legislación. Esta política se alinea con las **recomendaciones** para la minimización de riesgos de privacidad en los escritorios de trabajo:
  - No dejar contraseñas escritas en *pots-its* u otros sitios accesibles.
  - Bloquear todos los dispositivos del trabajo con contraseñas.
  - Limpiar la mesa de trabajo a final del día y archivar con llave los documentos sensibles.
  - No imprimir un documento si no es necesario y destruirlo después de hacer uso del mismo si no consideramos que deba ser archivado.
  - Usar cajones y archivadores que cierren con llave.
  - Formar a la plantilla en riesgos para la privacidad.

Materiales

Bibliografía básica

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.

Materiales en línea

Itziar de Lecuona y Genís Roca explican el nuevo RGPD (vídeo)

Entrevista de Xavier Grasset en el programa *Més 324* de *Televisió de Catalunya* a Genís Roca, Presidente de RocaSalvatella, y a Itziar de Lecuona, Profesora y Subdirectora del Observatorio de Bioética y Derecho de la Universidad 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)

Hoja de ruta sintética con 6 pasos para la adaptación del RGPD en nuestra organización.

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

Guía del RGPD para responsables de tratamiento (pdf)

Completa publicación conjunta de diversas agencias de protección de datos (estatal, catalana y vasca) para uso de responsables del tratamiento. Además de la descripción de los requisitos legales, incluye recomendaciones en cada uno de los apartados.

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

Reglamento general de protección de datos

Portal de la *Generalitat de Catalunya* que ofrece preguntas frecuentes y guías (entre ellas, una pensada para personas encargadas) sobre el cumplimiento del reglamento. Incluye una traducción (no oficial) del reglamento al catalán, además de las versiones castellana e inglesa.

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

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

Guía que delimita las funciones y responsabilidades de responsables y encargados, y ofrece pautas para una correcta elaboración y seguimiento de los contratos.

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.

Artículo que aclara cómo el RGPD no impide la captación activa de talento, pero sí regula cómo tiene que establecerse la comunicación y las autorizaciones explícitas que hacen falta para proseguirla.

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.

Artículo con un enfoque práctico y diferentes supuestos de aplicación. Incluye una comparación entre los antiguos requisitos de la LOPD y las nuevas obligaciones generadas por el RGPD

https://josefacchin.com/rgpd/

Mendieta, Carles. "Los límites de la Inteligencia Artificial: una mirada optimista con toques de alerta". *Blog Factor Humà*, 12/09/2018.

Debate sobre los límites de la Inteligencia Artificial entre Genís Roca, Presidente de *Roca Salvatella*, e Itziar de Lecuona, Subdirectora del *Observatorio de Bioética y Derecho de la UB* en el marco del acto de entrega de los *Premios Factor Humà*.

https://factorhuma.org/es/actualitat/blog-factor-huma/13704-los-limites-de-la-inteligencia-artificial-una-mirada-optimista-con-toques-de-alerta