COL·LEGI D'ACTUARIS DE CATALUNYA

La Protecció de Dades en les Entitats Asseguradores

a càrrec de

Sr. Albert Agustinoy Guilayn
Advocat, soci de Cuatrecasas

i

Sr. Jorge Monclús Ruíz
Advocat, associat sènior de Cuatrecasas

27 de juny de 2019, a les 18:00 hores, a les oficines de
Cuatrecasas, Av. Diagonal 191, Barcelona 08018

El Reglament General de Protecció de Dades (RGPD) i la recentment aprovada Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades de caràcter personal i garantia de drets digitals han definit el marc que qualsevol empresa i entitat ha de respectar pel que fa a l'àmbit de la privacitat. Després d'un temps d'aplicació d'ambdues normes, encara es persegueix una aplicació uniforme i coherent del dret de protecció de dades dins el territori de la Unió Europea, havent obligat a tot tipus d'empreses a revisar els seus procediments i documents legals per a la recollida i el tractament de les dades.

És en aquest context, que és important familiaritzar-se amb els criteris que les autoritats comunitàries i nacionals han vingut desenvolupant respecte d'aquest nou marc regulador, per tal de comprendre'l i assegurar el seu adient compliment donada la creixent importància d'aquesta sensible qüestió.

En aquesta sessió analitzarem les principals novetats i obligacions que recullen aquestes normes, amb un estudi detallat dins l´àmbit de les entitats asseguradores.

Cuatrecasas
Cuatrecasas és un dels despatxos jurídics capdavanters a la Península Ibèrica i està especialitzat en les diferents àrees del dret d'empresa.

El seu equip especialitzat en Assegurances i Previsió Social té una àmplia experiència en l'assessorament institucional, jurídic i fiscal, corresponent a entitats asseguradores, gestores de fons de pensions i mediadors d'assegurances, així com en l'assessorament relatiu als productes que aquelles entitats ofereixen en el mercat.

CUATRECASAS

LA PROTECCIÓN DE DATOS EN EL ÁMBITO DE LOS SEGUROS

ALBERT AGUSTINOY
JORGE MONCLÚS

Barcelona, 27 de junio de 2019

CUATRECASAS

COL·LEGI D'ACTUARIS DE CATALUNYA

Tres cuestiones fundamentales

- **CUÁNDO** → 25 de mayo y 7 de diciembre de 2018.
- **A QUIÉN** → A los responsables establecidos en la UE. Excepcionalmente, a responsables no establecidos en la UE.
- **ANTE QUIÉN** → Autoridad de control del establecimiento principal del responsable.

RESPONSABILIDAD PROACTIVA. PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

- El responsable debe establecer medidas apropiadas **para garantizar y poder demostrar que el tratamiento** de datos que realiza es conforme con el RGPD. Las medidas deben revisarse y actualizarse.

- **Protección de datos desde el diseño**: a la hora de establecer los medios para el tratamiento y durante el tratamiento, el responsable debe establecer medidas adecuadas para adecuarlo al RGPD y proteger los derechos de los interesados.

- **Protección de datos por defecto**: el responsable debe establecer medidas para garantizar que, por defecto, se traten únicamente los datos necesarios para los fines específicos del tratamiento. Esto afecta a la cantidad de datos recopilados, al alcance del tratamiento, al periodo de conservación y a la accesibilidad (por defecto, los datos no pueden hacerse accesibles a un número indeterminado de personas sin intervención de la persona).

MEDIDAS DE RESPONSABILIDAD PROACTIVA

- **Obligaciones** del responsable y del encargado del tratamiento

  - ✓ Determinar las medidas **técnicas y organizativas** apropiadas.
  - ✓ Evitar situaciones de discriminación, privación de derechos o libertades...
  - ✓ Cuando el tratamiento evalúe aptitudes personales, sea masivo...

- **Bloqueo de datos**

  - ✓ **Obligación de bloquear** los datos cuando deban rectificarse o suprimirse, hasta que prescriba la responsabilidad por el tratamiento.
  - ✓ Tras dicho plazo **deben destruirse.**
  - ✓ Consiste en la **identificación y reserva de los datos**, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización.
    - ➢ **Excepción**: para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, incluyendo la AEPD.

BASES JURÍDICAS

- La licitud del tratamiento depende de la concurrencia de las bases jurídicas que establece el RGPD:
  - ✓ Consentimiento (explícito en algunos casos).
  - ✓ Ejecución de contrato o aplicación de medidas precontractuales.
  - ✓ Cumplimiento de obligación legal.
  - ✓ Protección de intereses vitales.
  - ✓ Cumplimiento de misión realizada en interés público o en ejercicio de poderes públicos.
  - ✓ Interés legítimo.
- Todas las bases jurídicas tienen la misma importancia.
- Debe informarse de la base jurídica a los interesados.
- **Prohibición general** datos sensibles → **Excepción**: podrán tratarse datos relacionados con la salud y datos genéticos según lo dispuesto en la **Ley 20/2015**, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

DERECHO DE INFORMACIÓN

- En el momento de recogida/obtención de los datos debe informarse de:
  - Identidad y datos de contacto del responsable, representante y delegado.
  - Fines y base jurídica del tratamiento.
  - Destinatarios o categorías de destinatarios.
  - Transferencias a terceros países, indicando existencia o ausencia de decisión de adecuación de la Comisión, o referencia a las garantías adecuadas y forma de obtener una copia.
  - Plazo de conservación o, si no es posible, criterios para determinar el plazo.
  - Derechos de acceso, rectificación, supresión, oposición, limitación, portabilidad y, si hay consentimiento, derecho a retirarlo.
  - Derecho a presentar reclamación ante autoridad de control.
  - Si existe obligación legal o contractual de facilitar los datos, o son necesarios para suscribir el contrato; si es obligatorio facilitar los datos y las consecuencias de no facilitarlos.
  - Existencia de un mecanismo de decisión automatizado que comprenda la elaboración de perfiles indicando la lógica aplicada y la relevancia y consecuencias previstas del tratamiento.

DERECHO DE INFORMACIÓN

- **Información por capas**
  - Permite dar cumplimiento al deber de información a través de dos filtros: **información básica e información completa**.
  - Deberá indicarse un **método eficaz** de acceso al resto de la información.
- Si los datos se **obtienen directamente** del afectado
  - La identidad del responsable del tratamiento y de su representante (si tiene)
  - La finalidad del tratamiento
  - La posibilidad de ejercer sus derechos
  - Si se elaboran perfiles, deberá indicarse así como el derecho de oposición
- Si los datos **no se obtienen directamente** del afectado
  - La información básica anterior; y
  - Las categorías de datos objeto del tratamiento
  - Las fuentes de las que procedieran los datos

TRATAMIENTOS CONCRETOS (I)

- Listado no exhaustivo de supuestos a los que el legislador concede una presunción iuris tantum de licitud.

  - Tratamiento de **datos de contacto**, de empresarios individuales y de profesionales liberales.
  - Sistemas de **información crediticia**.
  - Tratamientos en **transacciones mercantiles**.
  - Tratamientos con fines de **videovigilancia**.
  - Sistemas de **exclusión publicitaria**.
  - Sistemas de información de **denuncias internas**.
  - Tratamiento de datos en el ámbito de la **función estadística pública.**
  - Tratamiento de datos con fines de **archivo en interés público** por parte de las Administraciones.
  - Tratamiento de datos relativos a **infracciones y sanciones administrativas**.

TRATAMIENTOS CONCRETOS (II)

- **TRATAMIENTO DE DATOS DE CONTACTO, DE EMPRESARIOS INDIVIDUALES Y DE PROFESIONES LIBERALES**
  - **Objeto**: únicamente datos de contacto y de función o cargo desempeñado.
  - **Requisitos**:
    - Que se trate únicamente datos necesarios para su localización.
    - Que la única finalidad sea la de mantener relaciones de cualquier índole.
- **TRATAMIENTO RELACIONADOS CON OPERACIONES MERCANTILES**
  - **Objeto**: datos que pudieran derivarse de las principales transacciones mercantiles (p. ej. modificaciones estructurales).
  - **Requisitos**: Que los datos sean necesarios para garantizar la operación y la prestación de servicios.
  - **Obligaciones**: Si la operación no se concluye, deberán suprimirse los datos de forma inmediata.

TRATAMIENTOS CONCRETOS (III)

- **TRATAMIENTOS CON FINES DE VIDEOVIGILANCIA**
  - **Finalidad**: preservar la seguridad de las personas, bienes e instalaciones.
  - **Requisitos**:
    - Solo grabar la vía pública si imprescindible. NUNCA: domicilio privado.
    - Suprimir datos en un mes desde su captación.
    - Instalar dispositivo informativo en lugar suficientemente visible.
- **SISTEMAS DE INFORMACIÓN DE DENUNCIAS INTERNAS**
  - **Objeto**: creación y mantenimiento de sistemas de información para la denuncia, incluso anónima, de actos y conductas contrarios a la normativa general o sectorial.
  - **Requisitos**:
    - Informar a los empleados de la existencia de estos sistemas.
    - Limitar el acceso a los responsables de control y excepcionalmente a terceros si se deben adoptar medidas disciplinarias.
    - Adoptar medidas de seguridad de confidencialidad.
    - Mantener los datos el plazo mínimo y, en todo caso, máximo tres meses.

DELEGADO DE PROTECCIÓN DE DATOS

- La LOPD prevé un listado de **sectores obligados a designar** DPD → las entidades aseguradoras y reaseguradoras.
- **Interlocutor** con la AEPD, **independiente e inamovible**, actuará en caso de reclamación ante la AEPD.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

- El **responsable** debe llevar un **registro de las actividades de tratamiento.**
- RAT & Documento de Seguridad: la extraña pareja.
- Por regla general, no aplicará a empresas de menos de 250 empleados.

NOTIFICACIÓN DE INFRACCIONES DE SEGURIDAD

- Como regla general, plazo máximo de 72 horas desde que tenga constancia.
- Notificación a los **interesados** cuando la violación tenga un alto riesgo para sus derechos y libertades

EVALUACIÓN DE IMPACTO

- Previamente a cualquier tratamiento que probablemente suponga un **alto riesgo** para los derechos y libertades de los interesados, el responsable debe evaluar el impacto de las operaciones de tratamiento.

- Obligatoria en los siguientes casos (ejemplos):

  - ✓ Evaluación sistemática y exhaustiva de aspectos personales basada en un tratamiento automatizado, a partir de la cual se toman decisiones que producen efectos jurídicos en relación con los particulares o les afectan significativamente.
  - ✓ Tratamiento a gran escala de categorías especiales de datos.
  - ✓ Observación sistemática a gran escala de una zona de acceso público.

- La autoridad de control puede determinar supuestos que requieran y no requieran evaluaciones de impacto. Deberá comunicarlo al CEPD.

- Si la evaluación de impacto indica que el tratamiento entraña un riesgo alto (a pesar de las medidas adoptadas), el responsable deberá consultar a la autoridad de control antes de proceder al tratamiento.

ENCARGO DE TRATAMIENTO (I)

- El responsable debe elegir un **encargado que ofrezca garantías suficientes.**

- Debe **regularse por contrato** (o acto jurídico equivalente), que deberá incluir:

  - ✓ Objeto, duración, naturaleza y finalidad del tratamiento, categorías de interesados y de datos personales, obligaciones y derechos del responsable y del encargado.

  - ✓ Obligaciones del encargado:

    - Garantizar el compromiso de confidencialidad de las personas con acceso a datos.
    - Implementar medidas de seguridad y ayudar al responsable a garantizar el cumplimiento de las obligaciones relativas a seguridad de los datos.
    - Asistir al responsable para atender los derechos de los interesados.
    - Poner a disposición del responsable información para probar el cumplimiento de sus obligaciones y permitir auditorías.
    - Informar inmediatamente al responsable si entiende que una instrucción vulnera la normativa de protección de datos.
    - Notificar violaciones seguridad.
    - Registro de actividades de tratamiento en nombre del responsable.

ENCARGO DE TRATAMIENTO (II) – sector asegurador

- Regulación en la **Ley 26/2006**, de 17 de julio, de mediación de seguros y reaseguros privados (art. 62):
  - ✓ Agentes de seguros exclusivos y operadores de banca-seguros exclusivos - encargados del tratamiento de la entidad aseguradora.
  - ✓ Agentes de seguros vinculados y operadores de banca-seguros vinculados - encargados del tratamiento de las entidades aseguradoras.
  - ✓ Corredores de seguros y de reaseguros - responsables del tratamiento respecto de los datos de las personas que acudan a ellos.
  - ✓ Auxiliares externos - encargados del tratamiento de los agentes o corredores de seguros con los que hubieran celebrado el correspondiente contrato mercantil.
- El régimen actual seguiría vigente con el RGPD, salvo modificación legislativa específica.
- Será preciso actualizar los contratos de agencia/encargo de tratamiento al nuevo RGPD.

MEDIDAS DE SEGURIDAD

- Las medidas de seguridad no están predeterminadas, sino que deben ser **adecuadas al riesgo** y tener en cuenta factores tales como el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento.

- Ejemplos: seudonimización; cifrado; medidas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; medidas para restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

- ¿Auditorías?: "verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento".

RÉGIMEN SANCIONADOR (I)

- Sanciones económicas:
  - ✓ Hasta 10M€ o hasta el 2% VN por incumplimiento obligaciones de responsable/encargado, de organismos de certificación y de autoridades de control.
  - ✓ Hasta 20M€ o hasta el 4% VN por vulneración de principios básicos, de los derechos de los sujetos y transferencias internacionales.
  - ✓ Hasta 20M€ o hasta el 4% VN por incumplimiento de las resoluciones de la AEPD
- Prescripción de las sanciones:
  - ✓ Sanciones < 40.000 € → 1 año
  - ✓ Sanciones 40.001-300.000 € → 2 años
  - ✓ Sanciones > 300.000 € → 3 años

RÉGIMEN SANCIONADOR (II)

- Sujetos responsables
  - Responsables y encargados del tratamiento y sus representantes → **responsabilidad solidaria**.
  - Entidades de certificación.
  - **Importante**: el DPO NO está sujeto a responsabilidad.

- Nuevos **criterios de graduación**
  - Afectación a los **derechos de los menores**.
  - Disponer de forma **voluntaria de DPO**.
  - Sometimiento voluntario del responsable o encargado a **métodos ADR** para la resolución de controversias entre ellos y los interesados.

INFRACCIONES

Muy graves

- ✓ Incumplimiento deberes:
  - ➢ Información
  - ➢ Confidencialidad
  - ➢ Bloqueo de datos
  - ➢ Colaboración con AEPD
  - ➢ Principios y garantías rectores
- ✓ Obstaculización reiterada del ejercicio de los derechos
- ✓ Tratamiento sin base lícita o para una finalidad distinta

Graves

- ✓ Incumplimiento deberes:
  - ➢ Realización EIPD
  - ➢ Notificación violación de seguridad a la AEPD
  - ➢ Disponer de RAT
  - ➢ Adopción medidas técnicas adecuadas
  - ➢ Encargo de tratamiento a un tercero sin contrato
- ✓ Obstaculización funciones del DPO
- ✓ Tratamiento sin consulta previa cuando sea preceptiva

Leves

- ✓ Incumplimiento deberes:
  - ➢ Contrato encargo
  - ➢ RAT incompleto
  - ➢ Transparencia en la información
  - ➢ Registro de violación de seguridad
  - ➢ Publicación datos de contacto DPO
- ✓ Omitir notificación
  - ➢ A afectados violación
  - ➢ rectificación o supresión datos
- ✓ Notificación tardía, incompleta AEPD

DERECHOS DIGITALES EN EL ÁMBITO LABORAL

- **Derecho a la intimidad** en el ámbito laboral
  - Uso de **dispositivos digitales** en el ámbito laboral
  - Uso de **dispositivos de videovigilancia** y de grabación de sonidos en el lugar de trabajo
  - Uso de **sistemas de geolocalización** en el ámbito laboral

- Derecho a la **desconexión laboral**
  - Deber de elaborar, previa audiencia con los representantes de los trabajadores, una **política interna** que establezca las modalidades de ejercicio de este derecho y actividades de sensibilización.
  - Finalidades:
    - Garantizar el tiempo de descanso
    - Evitar fatiga digital
    - Potenciar conciliación

RECOMENDACIONES

- Elaborar el registro de actividades del tratamiento.
- Adaptar las cláusulas informativas.
- Revisar aquellos tratamientos basados en el consentimiento que puedan verse afectados por la derogación del consentimiento tácito.
- Preparar adendas a aquellos contratos de prestación de servicios que impliquen un encargo de tratamiento.
- Valorar si hay tratamientos que se prevean realizar que puedan requerir una evaluación de impacto.
- Elaborar políticas internas para la atención de derechos, la realización de evaluaciones de impacto, la notificación de violaciones de seguridad...
- Valorar la necesidad o conveniencia de nombrar un DPO.
- … Llamar al abogado…

MUCHAS GRACIAS

albert.agustinoy@cuatrecasas.com

jorge.monclus@cuatrecasas.com

CUATRECASAS

COL·LEGI D'ACTUARIS DE CATALUNYA