ascobi bieba

Bilbao, a 17 de diciembre de 2018

Estimado asociado:

El 6 de diciembre de 2018 se publicó en el BOE la **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales,** quedando derogada la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal. Esta nueva Ley adapta y complementa lo dispuesto en el Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos, en vigor desde 2016 y de plena aplicación desde el 25 de mayo de 2018. Asimismo incorpora un novedoso Título X sobre garantía de derechos digitales.

A continuación se destacan los aspectos más relevantes de la nueva Ley Orgánica que tienen relación con el ámbito de la empresa y los Recursos Humanos:

1. Consentimiento: Es una de las bases legales del tratamiento, al mismo nivel que las restantes bases que recoge el Reglamento europeo. Debe consistir en una manifestación o una clara acción afirmativa del afectado, excluyéndose el consentimiento tácito y el presunto. Cuando dicho consentimiento se recabe para una pluralidad de finalidades, será necesario que conste otorgado de manera específica e inequívoca para todas ellas. La edad mínima para el consentimiento de los menores de edad será a los 14 años.

2. Derechos de los interesados: Se reproducen los ya previstos en el Reglamento europeo (acceso, rectificación, supresión o derecho al olvido, limitación, oposición y portabilidad) si bien los amplía añadiendo un especial derecho al olvido en búsquedas de internet y redes sociales y el derecho a la portabilidad en redes sociales.

3. Categorías especiales de datos: Se limita el consentimiento en el tratamiento de categorías especiales de datos, no siendo suficiente para el tratamiento de ciertas categorías de datos personales (ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico).

4. Responsables y Encargados de tratamiento: Se diferencia entre ambas categorías y se establecen las obligaciones y responsabilidades de ambos, y extiende la vigencia de los contratos de encargado del tratamiento suscritos con anterioridad a la aplicación del Reglamento europeo hasta su fecha de vencimiento o, en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022, si bien antes de esa fecha cualquiera de las partes podrá exigir la actualización del contrato al nuevo marco legal.

5. Transferencias internacionales de datos: Se desarrollan los supuestos en los que se permite realizar dichas transferencias.

6. Sistemas de videovigilancia: Se incorporan limitaciones y directrices formuladas por la Agencia Española de Protección de Datos en su guía sobre esta materia. Se regula la utilización de cámaras por parte de las empresas y administraciones con la finalidad de control de los trabajadores o empleados públicos, estableciéndose límites de uso y determinadas prohibiciones. Se regula la grabación de imágenes en el lugar de trabajo, siendo en general necesario informar al empleado y sus representantes, salvo casos de comisión de ilícitos, en que podría informarse a través de un cartel informativo general. Se excluye la posibilidad de grabación en los "lugares de ocio y esparcimiento" dentro de la empresa.

7. Sistemas de denuncias internas: Se establece la posibilidad de que se establezcan sistemas anónimos de denuncias en relación con la existencia de una vulneración de normativa general o sectorial aplicable al responsable. En materia de Códigos de Conducta, se potencian estas figuras de autorregulación conforme a lo establecido en el Reglamento europeo. Éstos podrán tener mecanismos de resolución extrajudicial de conflictos a los que las autoridades de control podrán remitir las reclamaciones formuladas por los interesados para su resolución alternativa a la tramitación de un procedimiento por aquélla.

8. Bloqueo de los datos: Se limita la finalidad del tratamiento de los datos bloqueados a su conservación y puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes durante los plazos de prescripción de las acciones derivadas del tratamiento. Caben medidas alternativas en caso de imposibilidad técnica o coste desproporcionado del bloqueo, tales como el copiado seguro de los datos a través de sistemas que impidan su manipulación.

9. El Delegado de Protección de Datos: Se potencia esta figura y se incluye el listado de supuestos en los que se considera obligatoria la designación de dicho delegado, así como la cualificación de la que debe disponer y sus funciones. Se debe notificar el nombramiento a la Agencia Española de Protección de Datos en el plazo máximo de diez días.

10. Régimen sancionador: Se cualifican las infracciones tipificadas en el Reglamento europeo como muy graves, graves y leves a los solos efectos de determinar sus plazos de prescripción. Asimismo introduce criterios de graduación complementarios de los establecidos en el Reglamento europeo, reproduciéndose las normas de procedimiento que ya establecía el Real Decreto-Ley 5/2018, de 27 de julio. Se exime de las sanciones económicas a las administraciones públicas que incumplan la normativa.

11. Derechos digitales: Se reconoce y garantiza un nuevos derechos digitales entre los que destacan:

- **Derecho de acceso universal a internet**: Se garantiza un acceso universal, asequible, de calidad y sin discriminación alguna para toda la población.

- **Derecho a la seguridad digital**: Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de internet.

- **Derecho a la educación digital**: Se garantiza en el sistema educativo la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales seguro y respetuoso con los valores constitucionales, los derechos fundamentales y la dignidad humana, así como la garantía de la intimidad personal y familiar y la protección de datos personales.

- **Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral**: Los trabajadores y los empleados públicos tienen derecho a la protección de su intimidad en el uso de los dispositivos digitales. El empleador podrá acceder a los contenidos derivados del uso de los medios digitales facilitados al trabajador sólo a efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de estos dispositivos. Será obligatorio que cada empresa establezca, con la participación de los representantes de los trabajadores, los criterios de utilización de los dispositivos digitales, respetando los estándares mínimos de protección de su intimidad e informe de estos criterios a los trabajadores; determinando, por ejemplo, los periodos durante los cuales el empleado pueda hacer uso personal de estas herramientas, en caso de estar permitido.

- **Derecho a la desconexión digital de los trabajadores y empleados públicos**: Con el fin de garantizar que fuera del tiempo de trabajo legal o convencionalmente establecido se respeta el tiempo de descanso, permisos y vacaciones, así como su intimidad personal y familiar. El ejercicio de este derecho estará sujeto a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y la representación de los trabajadores. El empleador, previa audiencia de los representantes de los trabajadores, deberá elaborar una política interna en la que definirá las modalidades del ejercicio del derecho a la desconexión y las acciones de formación y sensibilización de los trabajadores sobre el uso razonable de las tecnologías.

- **Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo:** Los empleadores podrán tratar las imágenes obtenidas para el ejercicio de las funciones de control de los trabajadores previstas en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de la función pública, previa información a los trabajadores o empleados públicos y, en su caso, a sus representantes de la existencia de cámaras de videovigilancia y el posible uso de sus imágenes para el control laboral. Asimismo se establece que el uso de sistemas de grabación de sonido deberá ser también comunicado y sólo será posible cuando concurran riesgos para la seguridad de las instalaciones, bienes y personas, derivado de la actividad en el centro de trabajo.

- **Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral:** Los empleadores podrán tratar los datos obtenidos para el ejercicio de las funciones de control de los trabajadores previstas en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, previa información de la existencia y características de estos dispositivos a sus representantes.

- **Derechos digitales en la negociación colectiva**: Dado que los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los empleados y la protección de derechos digitales en el ámbito laboral.

12. Datos de personas fallecidas: Los herederos y las personas vinculadas al fallecido por razones familiares o de hecho, salvo prohibición expresa por el fallecido o por ley, podrán ejercitar los derechos de acceso, rectificación o supresión respecto de los datos del fallecido. De igual forma, podrán ejercer los derechos mencionados el Ministerio Fiscal y/o los representantes legales respecto de los menores fallecidos y el personal de apoyo de personas fallecidas con discapacidad.

El presente Real Decreto entró en vigor el día siguiente a su publicación, esto es, el 7 de diciembre de 2018.