Expansión | JURÍDICO

PROTECCIÓN DE DATOS GUÍA PARA ADAPTARSE AL NUEVO REGLAMENTO

¿Cómo se gestionan los datos personales de los trabajadores?

La aplicabilidad del Reglamento General de Protección de Datos, a partir del 25 de mayo, supone una transformación en la gestión de la información personal que los trabajadores facilitan a la empresa.

Agustín Born. Madrid

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea basa sus principios fundamentales en los que hasta ahora se venían aplicando en nuestro país, pero aun así, hay cambios que afectan no sólo a las empresas, sino también a sus trabajadores, que deberán modificar su aproximación a la privacidad.

En primer lugar, está la formación que todos los empleados deben recibir antes del 25 de mayo y que implica la obligatoriedad a la hora de conocer todas las novedades. Como indica Cecilia Álvarez, presidenta de la Asociación Profesional Española de Privacidad (APEP), se trata de un cambio de mentalidad que empieza por la dirección y que debe incorporar "el respeto a la privacidad de los clientes o de otros compañeros, como un elemento esencial de cualquier estrategia corporativa y que debe quedar reflejado en los procesos, la tecnología y la documentación interna".

Todos los departamentos de la empresa y sus trabajadores, dependiendo del grado de exposición a la privacidad, se verán afectados. "Las actividades de perfilado y márketing directo son consideradas como actividades de riesgo, por ejemplo. Deberán revisarse no sólo los procesos y tecnología utilizada a efectos comerciales, sino también verificar los bonus u otros incentivos económicos del departamento comercial", indica la presidenta de la APEP.

Los departamentos de recursos humanos, los de *compliance* o las asesorías jurídicas de las empresas realizan igualmente tratamiento de datos personales con gran impacto en los procesos de las organizaciones, asumiendo una carga de trabajo más especializada y la necesidad de contar con expertos en protección de datos.

Dreamstime

El RGPD también afecta a la utilización de la información facilitada por la plantilla.

Las compañías tendrán que revisar los bonus y los incentivos de los comerciales

Los empleados están obligados a comunicar si advierten cualquier tipo de fuga de datos

Nuevo procedimiento de información

Cuando sea el propio empleado quien recoja datos de carácter personal, como ocurre, por ejemplo, en la recepción de un hotel, no bastará con que se exhiba el documento para recabar el consentimiento. "La entrada en vigor del RGPD obliga, además, a informar de otros elementos básicos como el responsable del tratamiento, legitimidad, finalidad, derechos ARCO o la denominada información de primera capa", indica Bárbara Román, socia de NoLegaltech. Una nueva circunstancia se produce en caso de que "sea el propio trabajador quien advierta una fuga de datos o una brecha de seguridad en el sistema, ya que estará obligado a informar al DPO o a su jefe inmediato", dependiendo del caso y según el protocolo que se establezca por el empleador en cumplimiento de la norma.

El RGPD para autónomos y 'freelance'

El RGPD provoca un cambio en el artículo 2.2 de la LOPD en lo que se refiere a los datos de contacto de los trabajadores autónomos y profesionales que prestan un servicio a una empresa y que la ley consideraba fuera del ámbito de aplicación del reglamento en España. Sin embargo, el reglamento europeo se aprueba sin hacer referencia ni excepción a este supuesto, por lo que se entiende de aplicación la norma europea superior. El proyecto de ley de excepción para el consentimiento requiere informar pero no tener el consentimiento previo, ya que entiende que existe una relación mercantil entre las dos partes y que existe un interés legítimo entre ambas.

Alonso Hurtado, socio de Ecija, explica que "el hecho de recabar el consentimiento previo para fines e intereses comerciales está ahora encima de la mesa y en revisión por la 'E-privacy regulation' de la UE (regulación de privacidad electrónica), que desmantela el actual modelo de negocio de las agencias de medios regulando los sistemas de gestión de 'cookies' y de las campañas de publicidad programática".

CASOS PRÁCTICOS

Fotos en la web

La imagen del trabajador es indudablemente un dato de carácter personal, y aunque no se enmarca en la categoría especial de datos, existe diferente casuística en el tratamiento que de ella puede hacerse. Jesús Mercader, catedrático de derecho del trabajo y socio de Sagardoy, establece diferentes situaciones en su obra 'Protección de datos en las relaciones laborales'. Así, la inclusión de una fotografía en las tarjetas identificativas estaría legitimada por motivos de seguridad o para la necesaria identificación del personal que realiza una actividad, mientras que la captación de fotos de clientes o la publicación de imágenes en la web corporativa de miembros de la empresa requerirá un consentimiento expreso porque tienen una función de promoción y calidad del servicio.

Videovigilancia

La videovigilancia pasa a tener un tratamiento de monitorización sistemática a partir del 25 de mayo. "El reglamento indica que el empleador tiene derecho a controlar al empleado, aunque siempre manteniendo los principios de proporcionalidad, idoneidad e información", indica Alonso Hurtado, socio de Ecija. En este sentido, apunta la resolución del TEDH en el llamado 'caso Köpke', cuando consideró inadmisible el recurso porque el uso que había hecho la empresa alemana en la que trabajaba era proporcionado a las circunstancias del caso: se habían detectado pérdidas; la conducta de la demandante y de otro empleado eran sospechosas y fueron sólo ellos objeto de vigilancia; la medida fue limitada en el tiempo y "sólo había cubierto el área que rodea la caja y era accesible para el público", como indica la sentencia.

Dreamstime

Evaluación y productividad

Existen numerosos casos de uso de datos de los trabajadores derivados de la dinámica laboral propiamente dicha: gestión de nóminas, registros de actividades laborales o comunicaciones personales. Pero especialmente sensible resultan las relativas a la publicación y comunicación de las evaluaciones del trabajador, que en cualquier caso requieren del consentimiento expreso por parte del interesado. Se trata de comunicación verbal de resultados obtenidos por una persona, el archivo de esta información o su publicación en la intranet corporativa. Cuestiones todas ellas sobre las que la propia Agencia Española de Protección de Datos (AEPD) se ha pronunciado en varias ocasiones.

Biometría

Los datos biométricos, como huellas dactilares, estructura facial y otros identificadores únicos cada vez más extendidos como llave de acceso a servicios y accesos, están considerados como datos especialmente sensibles. Como indica Hurtado, "podría defenderse un interés legítimo en su uso siempre que sólo sea para el fin que se destina, pero también que una simple tarjeta magnética cumple la misma función en algunos casos sin que la utilización sea tan intrusiva".