"Una manera de hacer europa"

Fondo Europeo de Desarrollo Regional

UNIÓN EUROPEA

PROGRAMA OFICINAS DE TRANSFORMACIÓN DIGITAL

Cofinanciado por el Programa Operativo Plurirregional de España (POPE) (C-027/17-ED)

Guía para la gestión correcta de la protección de datos en relación con el Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y lucha contra la precariedad laboral en la jornada de trabajo

Creada con la colaboración de Compliance-Spain

Compliance-Spain
Cumplimiento Normativo

Compliance-Spain
Cumplimiento Normativo

Guía para la gestión correcta de la protección de datos en relación con el Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y lucha contra la precariedad laboral en la jornada de trabajo

Nota previa: esta guía no entra a valorar cuestiones de derecho laboral para lo cual FREMM pone a disposición de los socios su servicio de asesoría laboral.

Antecedentes

El Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y lucha contra la precariedad laboral en la jornada de trabajo, viene a regular el registro de la jornada laboral, como medida para combatir la precariedad en el trabajo, ya que la realización de más horas de las pactadas en el contrato supone dos afectaciones: el salario y la dificultad de conciliar la vida personal. Asimismo, la creación de este registro asegura la conformidad de la normativa española con el ordenamiento europeo.

Exactamente este cambio normativo viene establecido en el artículo 10 del citado RDL, que modifica el texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, a los efectos de garantizar el cumplimiento de los límites en materia de jornada, de crear un marco de seguridad jurídica tanto para las personas trabajadoras como para las empresas y de posibilitar el control por parte de la Inspección de Trabajo y Seguridad Social.

Para facilitar el conocimiento de la información que se facilita a través de esta guía, es preciso detenernos brevemente en una serie de conceptos que, a pesar de ser básicos, es necesario tener siempre presente en todo caso que estemos hablando de la normativa referente a la protección de datos de carácter personal.

¿Qué es un fichero de datos personales?

Un fichero es todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso; de aquí que podamos realizar una primera gran distinción:

Los ficheros no automatizados consisten en conjuntos de datos personales organizados de forma no automática y estructurados conforme a criterios específicos relativos a personas físicas que permitan acceder sin esfuerzos

desproporcionados a sus datos personales, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Los ficheros automatizados consisten en conjuntos de datos organizados de forma automática y gestionados mediante, programas, soportes, y equipos informáticos.

¿Es cierto que existen distintos niveles de seguridad según el tipo de datos personales que trate la empresa?

Es correcto. Con la anterior normativa, **Real Decreto 1720/2007, de 21 de diciembre, por el que se aprobaba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal**y en función de las tipologías de datos personales que se trataran se debían aplicar una serie de medidas de seguridad sobre dichos datos. Cuanto más alto el nivel de seguridad, le supondrá un mayor coste la gestión de dichos datos, ya que deberá aplicar medidas más severas y rigurosas para su captación, almacenamiento, gestión y destrucción.

Nivel de seguridad alto. En esta categoría están todos los ficheros de datos personales y tratamientos de datos personales sobre ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico. Se aplica también a los datos personales con fines policiales recabados sin consentimiento del afectado y los derivados de violencia de género.

Nivel de seguridad medio. En esta categoría están todos los ficheros de datos personales y tratamientos de datos personales sobre comisión de infracciones administrativas o penales, prestación de servicios de solvencia patrimonial o de crédito, los relativos a potestades tributarias de la Administración, los relativos a servicios financieros y de mutuas de accidentes de trabajo, los que ofrezcan información sobre la personalidad y el comportamiento, y los operadores de comunicaciones electrónicas respecto de los datos de tráfico y localización.

Nivel de seguridad bajo. En esta categoría están todos los ficheros de datos personales y tratamientos de datos personales sobre el resto de datos que no se engloben en las categorías anteriores. También se aplica sobre datos relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual cuando:

a) Cuando los datos se utilicen al único fin de realizar una transferencia dineraria a entidades de las que los afectados son miembros.

b) Cuando se trate de ficheros o tratamientos de este tipo de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero.

c) Cuando se trate de ficheros o tratamientos que contengan datos de salud que se refieran exclusivamente al grado de discapacidad o a la condición de invalidez con motivo del cumplimiento de deberes públicos.

¿Continúa siendo válida esta distinción bajo la nueva normativa aplicable?

La respuesta es no.

De la nueva normativa aplicable en el tratamiento de datos de carácter personal, Reglamento general de protección de datos (RGPD) y en la LO 3/2018 (LOPDGDD), resultan dos categorías de datos:

1. Los que podríamos denominar datos de categoría ordinaria y,

2. Datos de categorías especiales.

¿Cuál es la mayor diferencia entre los datos de naturaleza ordinaria y los de naturaleza especial?

Podemos afirmar que, con carácter general, por un lado, todo dato de carácter personal que no sea de naturaleza especial se considera ordinario y, por otro, el tratamiento de los datos personales de categoría especial o sensible **está expresamente prohibido**, a menos que se permita su tratamiento en situaciones específicas contempladas en el Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del RGPD al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

El artículo 9 del RGPD regula el tratamiento de categorías especiales de datos personales, señalando la prohibición general de tratar ese tipo de datos. Ahora bien, el citado precepto delimita asimismo las circunstancias en las que estará permitido efectuar el tratamiento de esos datos especialmente sensibles.

Así, conforme lo dispuesto en el apartado 1º del artículo 9, quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, **datos biométricos dirigidos a identificar de manera unívoca a una persona física,** datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

Como vemos, el RGPD incluye dos nuevas categorías especiales de datos (datos genéticos y datos biométricos) que anteriormente no se encontraban expresamente contemplados en la normativa derogada. Estos datos son:

- Los datos genéticos y, los datos biométricos.

¿Qué es un datos biométrico?

Son aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de esta persona (imágenes faciales, datos dactiloscópicos, voz, firma, etc.).

¿Tiene esto importancia a los efectos del registro de la jornada laboral?

Sí. Tal y como veremos posteriormente, según sea el sistema que la empresa implante para llevar a cabo el control horario podremos encontrarnos ante el tratamiento de datos de naturaleza biométrica.

¿Qué tipo de ficheros se pueden generar para el tratamiento de los datos de carácter personal con ocasión del cumplimiento del Real Decreto-ley 8/2019, de 8 de marzo?

Como hemos visto anteriormente, se pueden generar dos tipos de ficheros:

1. No automatizados (papel).

2. Automatizados (electrónicos)

3. Mixtos (parte del fichero en papel y parte en soporte electrónico)

¿Qué pasos se han de dar para cumplir con la normativa de protección de datos?

Sin perjuicio de que posteriormente se entre más en detalle a su estudio, con carácter general el empresario deberá tomar en consideración y decidir sobre los siguientes aspectos:

1. Tipo de tratamiento que va a implementar.
2. Categoría de datos personales que serán objeto de tratamiento.
3. Elaboración de un registro de actividades de tratamiento.
4. Elaboración de un análisis de riesgos.
5. Elaboración de una evaluación de impacto en protección de datos.

6. Redacción y firma de contratos de encargo de tratamiento con proveedores de sistemas de control laboral.
7. Información a los empleados del nuevo tratamiento de datos.
8. Firma de acuerdos de confidencialidad.
9. Elaboración protocolos de acceso a la información almacenada.
10. Verificación periódica integridad del sistema.

Pasaremos a continuación a examinar más en profundidad cada uno de los puntos anteriores.

1. TIPO DE TRATAMIENTO QUE SE VA A IMPLEMENTAR

Como ya hemos visto, se ha de decidir si el tratamiento del registro horario de la jornada laboral se va a llevar a cabo mediante papel o mediante sistemas informáticos.

2. CATEGORÍAS DE DATOS PERSONALES QUE SERÁN OBJETO DE TRATAMIENTO.

Como regla general, tanto si se utiliza papel o medios electrónicos, los datos a tratar serán de naturaleza ordinaria (en contraposición a los de categoría sensible o especial): nombre, apellidos, número de empleado e, incluso, DNI o NIE.

¿Y si quiero utilizar la huella dactilar?

Nos encontraríamos ante el tratamiento de un dato de carácter personal de naturaleza biométrica, por definición, de categoría especial.

¿Quiere esto decir que está prohibido el uso de la huella dactilar para el control de la jornada laboral?

No. El uso de la huella dactilar está permitido, siempre y cuando se cumplan una serie de requisitos.

Explicación:

El uso de las nuevas tecnologías en el registro de jornada de los trabajadores puede hacerse siempre y cuando se cumplan con una serie de determinadas garantías, entre las que destacan la aplicación del principios de proporcionalidad, finalidad y minimización.

¿De dónde surge la legitimación del empresario para el tratamiento de estos datos biométricos?

La legitimación jurídica para el empresario sería el contrato laboral y la potestad laboral de la ejecución del contrato que se encuentra en los artículos 20 y 34 del Estatuto de los Trabajadores que establece al empleador garantizar del registro de la jornada laboral.

3. ELABORACIÓN DE UN REGISTRO DE ACTIVIDADES DE TRATAMIENTO.

Con la entrada en vigor del RGPD el 25 de mayo de 2018, ha desaparecido la obligación de elaborar y mantener el denominado Documento de Seguridad.

Este Registro de Actividades de Tratamiento (en adelante RAT) viene a unificar en un solo soporte tanto la necesidad de inscribir los ficheros ante la Agencia Española de Protección de Datos; como el mantenimiento del anteriormente denominado *Documento de Seguridad;* toda vez que el *Registro de actividades de tratamiento* incluirá entre otras cuestiones las medidas de seguridad.

¿Están todos los empresarios obligados a elaborar un RAT?

La respuesta es Sí.

En la práctica casi todas las empresas deben llevar uno, no sólo porque facilita acreditar ante los servicios de inspección de la AEPD que **su tratamiento de datos cumple** con los principios establecidos por el RGPD, sino porque además es difícil caer fuera de alguno de los siguientes supuestos:

a) Si la empresa tienes **más de 250 empleados**.
b) Si la empresa tiene **menos de 250 empleados** y además:
   - Si el **tratamiento** incluye **categorías especiales de datos** (origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, **afiliación sindical,** datos genéticos, **datos biométricos para identificar a una persona**, datos de salud, vida y orientación sexual).
   - Cuando se realice tratamiento de datos que puedan entrañar un **riesgo para los derechos y libertades de los interesados**.
   - El tratamiento de datos que se realiza se refiere a **condenas o infracciones penales**.
   - Cuando el **tratamiento de los datos no sea ocasional**.

Nota: se considera que el tratamiento de datos no es ocasional, entre otros supuestos si se tratan datos de:

- Clientes.
- Proveedores
- Personal (recursos humanos)

¿Dispongo de un documento de seguridad bajo la anterior normativa?, ¿me sigue sirviendo bajo la nueva Ley?

No, es necesario adaptar a la nueva normativa esos procesos y, reunificar en el nuevo RAT los ficheros inscritos y el documento de seguridad.

¿Cuál es el contenido básico de un *Registro de actividades de tratamiento*?:

Existen ligeras diferencias si el RAT lo lleva en calidad de Responsable o Encargado del tratamiento; pero con carácter general es necesario que contemple:

- Nombre y datos de contacto del responsable y, en su caso del corresponsable, representante del responsable y del delegado de protección de datos.
- Finalidades del tratamiento.
- Categoría de interesados y categoría de datos personales.
- Categoría de destinatarios a quienes se comunicaron o comunicarán datos personales, así como, terceros países u organizaciones internacionales.
- Transferencias de datos personales a un tercer país o una organización internacional.
- Plazos previstos para la supresión de los datos, cuando sea posible.
- Descripción general e las medidas técnicas y organizativas de seguridad.

Si la empresa actúa como **Encargado del tratamiento**se deberá llevar, además, un registro de las actividades de tratamiento efectuadas por cuenta del Responsable.

¿Ya dispongo de un fichero de gestión de personal/recursos humanos, estoy cumpliendo la Ley?

Si dentro de las finalidades de ese fichero no figura la del control de la jornada laboral la respuesta es **no**.

¿En ese caso, qué se ha de hacer?

Tal y como estamos viendo, habrá que crear un RAT nuevo, que registre este tratamiento o, si es un tratamiento ya existente, modificar los que ya teníamos de RRHH y añadir el control horario de los empleados.

¿Algo más?

Nuestra recomendación, en el caso de que se quiera implementar un control de jornada laboral mediante huella dactilar, es el de crear en todo caso un nuevo tratamiento específico y desde luego, como se verá posteriormente, informar al trabajador.

4. ELABORACIÓN DE UN ANÁLISIS DE RIESGOS.

¿Qué es un análisis de riesgos?

Uno de los requerimientos que establece el Reglamento General de Protección de Datos (RGPD) para responsables y encargados del tratamiento que realizan o desean realizar actividades de tratamiento con datos personales es la **necesidad de llevar a cabo un análisis de riesgos de la seguridad de la información** con el fin de establecer las medidas de seguridad y control orientadas a cumplir *los principios de protección desde el diseño y por defecto* que garanticen los derechos y libertades de las personas.

Ante la constante evolución tecnológica y los procesos de transformación digital que sufren las actividades de tratamiento de los datos personales, es crucial abordar dichos procesos desde un modelo enfocado en la **gestión continua del riesgo**, definiendo desde el diseño las medidas de control y seguridad necesarias para que el tratamiento nazca respetando los requerimientos de privacidad asociados al nivel de riesgo al que está expuesto y evaluando de forma periódica la efectividad de las medidas de control implantadas.

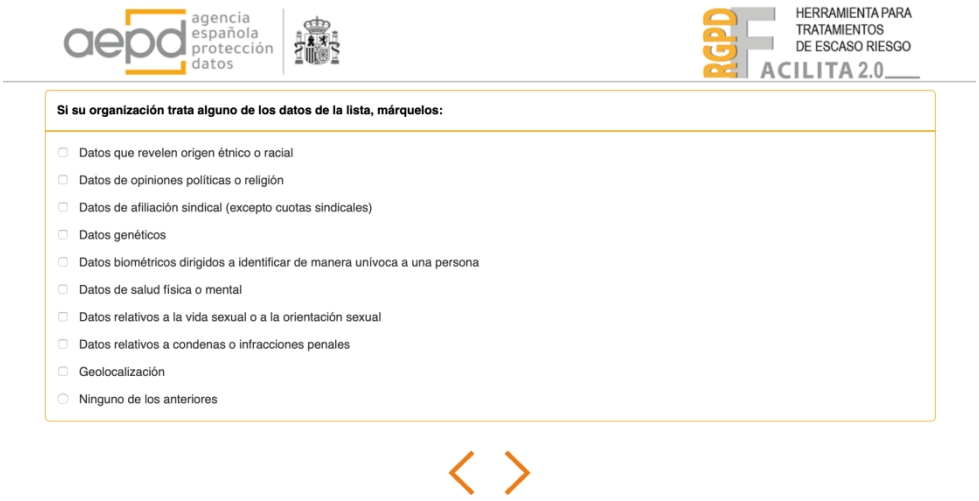
¿Debo llevar a cabo un análisis de riesgos para cumplir con la normativa de protección de datos en relación con el control de la jornada laboral?

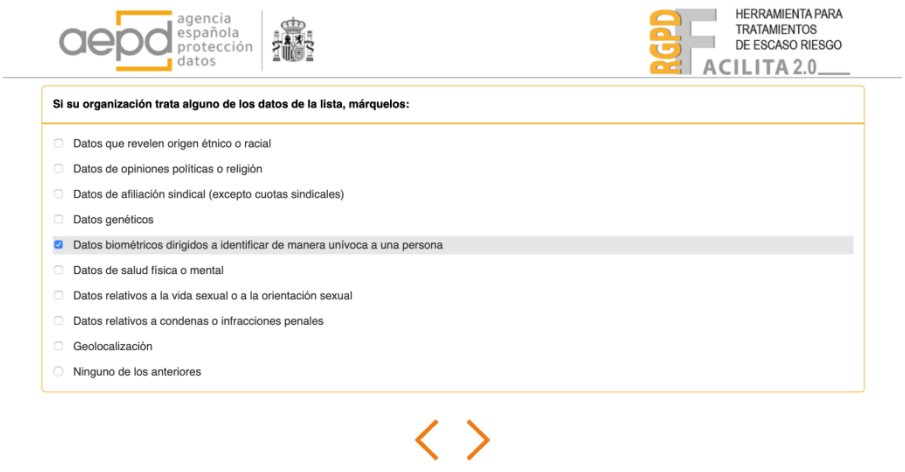
Sólo en el caso de que el control de la jornada laboral se lleve a cabo mediante el tratamiento de datos biométricos.

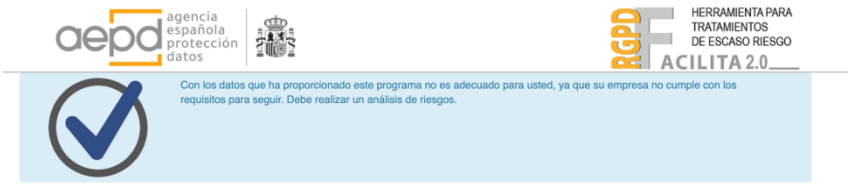
¿Se puede usar la herramienta FACILITA de la AEPD para hacer un análisis de riesgos en protección de datos?

Sí, exceptosi el control de la jornada laboral se lleva a cabo mediante el tratamiento de datos de naturaleza biométrica.

Efectivamente, si accedemos a la herramienta FACILITA de la web de la Agencia Española de Protección de Datos nos encontramos, tal y como se ve a continuación, que la herramienta nos indica que es preciso realizar un análisis de riesgos más profundo.







¿Qué persigue por tanto la realización de un análisis de riesgos?

Un análisis de riesgos busca garantizar en el tratamiento de datos de carácter personal:

- Confidencialidad.
- Integridad.
- Disponibilidad.
- Eficacia de las medidas adoptadas.
- Licitud de los tratamientos.

5. ELABORACIÓN DE UNAEVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS.

¿Es lo mismo una evaluación de impacto en protección de datos que un análisis de riesgos?

No.

Como ya hemos visto, el objetivo de un análisis de riesgos es determinar, desde el punto de vista de protección de datos, si un determinado tratamiento puede suponer un riesgo elevado (principalmente para los derechos y libertades individuales).

Sin embargo, el objetivo de una evaluación de impacto en protección de datos es **permitir a los responsables del tratamiento tomar medidas adecuadas** para reducir dicho riesgo (minimizar la probabilidad de su materialización y las consecuencias negativas para los interesados).

¿Debo llevar a cabo una evaluación de impacto en protección de datos para gestionar el control de la jornada laboral?

La respuesta es **No**, salvo que la misma se lleve a cabo mediante tratamiento de datos de naturaleza biométrica (huella dactilar, mano, firma, voz, iris, etc), pues por definición legal implica un alto riesgo así como el uso de una tecnología considerada especialmente invasiva.

6. REDACCIÓN Y FIRMA DE CONTRATOS DE ENCARGO DE TRATAMIENTO CON PROVEEDORES DE SISTEMAS DE CONTROL LABORAL.

¿Es necesario disponer de un contrato de encargo de tratamiento en todos los casos?

La respuesta es **No.**

¿En qué casos sí es necesario?

Por ejemplo, en el caso de control de jornada laboral mediante huella dactilar, si éste se presta a través de un software de un tercero que pueda tener acceso a la información recopilada tendremos que firmar un contrato de prestación de servicio de encargado de tratamiento correspondiente.

¿Está mi empresa protegida de riesgos legales si el proveedor del software dispone de unas condiciones generales?

No en todos los casos.

Cuanto más cumplan las condiciones generales del proveedor externo los requisitos del artículo 28 del RGPD, relativo al contrato de encargo de tratamiento, más cubierto estará jurídicamente la empresa.

Todo contenido dispuesto unilateralmente por el proveedor, al estilo de las condiciones generales de la contratación, irán en perjuicio de la empresa que asumirá la responsabilidad que se pudiera derivar en cuanto el mismo se separe de lo contemplado en el mencionado artículo 28. En casos extremos, dicha responsabilidad podría incluso afectar al proveedor, al pasar su posición de encargado de tratamiento al de responsable del mismo.

Pero, **¿cómo es posible que mi empresa asuma responsabilidad si he contratado una empresa externa para la gestión del control de la jornada de trabajo y tiene unas condiciones generales publicadas en su web?**

Deriva del artículo 28 del RGPD que manifiesta que "el responsable del tratamiento **elegirá únicamente**un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas , de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

A su vez, en el considerando 81 del RGPD se añade que , en particular , el responsable atenderá a los conocimientos especializados , fiabilidad y recursos del encargado de tratamiento, de cara a la aplicación de las medidas técnicas y organizativas que cumplan los requisitos del Reglamento.

¿Qué hago si la empresa con la que quiero contratar no quiere modificar o adaptar o incluir el contrato de encargo de tratamiento dentro de sus condiciones generales de servicio?

Sólo caben dos posibilidades:

a) Elegir otro proveedor.

b) Solicitar, con objeto de documentar que la empresa acredita la necesaria diligencia debida en la elección del encargado del tratamiento un **certificado o declaración responsable** en el que se manifieste expresamente que el proveedor, en el tratamiento de los datos que vaya a realizar se llevará a cabo conforme al Reglamento (UE) 2016/679 y a la LOPDyGDD 3/2018 de 5 de diciembre y que tendrá, entre sus fines, proteger adecuadamente los derechos de las personas afectadas.

7. INFORMACIÓN A LOS EMPLEADOS DEL NUEVO TRATAMIENTO DE DATOS.

Desde la propia AEPD (Agencia Española de Protección de Datos) se indica que no hace falta pedir el consentimiento al empleado para el uso dela huella dactilar, pero **sí es necesario** que el empleador informe sobre el tratamiento y finalidades de ese control horario.

Sobre esta cuestión ya han tenido oportunidad de pronunciarse tanto el Tribunal Supremo (STS 2/07/2007) y jurisprudencia de suplicación (STSJ Murcia 25/01/2010), como la Agencia de Protección de Datos (entre otros, Informe 0324/2009), estableciendo claramente la licitud de estos sistemas al tratarse de medidas adecuadas, pertinentes y no excesivas, estando limitadas a la mera identificación de los empleados para el cumplimiento del control horario. No existirá intromisión ilegítima en la intimidad de los empleados, siempre y cuando exista una advertencia e información previa tanto de su

instalación como de los motivos de su implantación, haciendo especial mención de su uso para el control laboral. En estos casos, si bien se exigen información previa, no será necesario el consentimiento expreso del trabajador cuando “el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales” (ex artículo 6.1 del RGPD) o en aquellos casos en los que “el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento” o, en algunos casos, cuando “el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales”

8. FIRMA DE ACUERDOS DE CONFIDENCIALIDAD.

Podemos considerar al contrato de confidencialidad como aquel documento firmado entre la empresa y un trabajador/proveedor cuyo objetivo principal es que estos últimos guarden secreto y reserva sobre determinada información que evite su divulgación o uso indebido durante la relación laboral /de prestación de servicios y que sigue vigente una vez terminada la misma.

¿Tengo que firmar acuerdos de confidencialidad con los trabajadores de mi empresa?

Sí.

¿Tengo que firmar acuerdos de confidencialidad con los proveedores de mi empresa?

Sí.

Es posible queel acuerdo de confidencialidad entre responsable y encargado forme parte del contrato de prestación de servicios. Por lo que habrá que estar a lo que se diga en el contrato.

Explicación

En el artículo 5 del RGPD se definen los principios relativos al tratamiento de datos personales entre los que se encuentran los relativos a la integridad y confidencialidad de los datos. La citada norma alude también a la confidencialidad en otros artículos como el 28, relativo al Encargado del tratamiento y el 32, que se refiere a la seguridad del tratamiento.

En el artículo 6 de la LOPyGDD, se dice que l*os responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de éste estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1 f) del Reglamento (UE) 2016/679.*

Código penal, artículos 197 y siguientes, se regula el delito de revelación de secretos, con penas de privación de libertad importantes.

9. ELABORACIÓN PROTOCOLOS DE ACCESO A LA INFORMACIÓN ALMACENADA.

Con carácter general es conveniente, como medida que acredita que la empresa tiene una posición proactiva con el tratamiento de datos de carácter personal disponer de uno o varios protocolos de tratamiento de datos.

Estos protocolos, persiguen garantizar la **confidencialidad, integridad y legalidad** en el tratamiento de esos datosy además, podrán contemplar aspectos relativos a:

- Uso de internet, correo electrónico y teléfono.
- Uso de dispositivos móviles.
- Confidencialidad de la información tratada.
- Régimen de instalaciones de programas de ordenador ajenos a la empresa.
- Control de accesos.
- Contraseñas de los equipos dedicados a la empresa.
- Copias de seguridad.
- Destrucción de la documentación.
- Uso de soportes informáticos y documentos fuera de la empresa.
- Etc.

¿Hasta que punto tiene este protocolo importancia?

Puede ser la diferencia entre que una sanción laboral pueda entenderse procedente o improcedente.

Ya dispongo de un protocolo de protección de datos en la empresa ¿qué tengo que hacer?

A los efectos del control del registro de la jornada laboral, hay que comprobar que este tratamiento de datos se encuentra contemplado y, en caso contrario, incluirlo.

Entonces, ¿qué debe recogerse en ese protocolo?

- Deberemos identificar quién tendrá la responsabilidad interna de gestionar estos datos, ya que sólo deberá hacerse por personal autorizado.
- Se deberá contemplar cómo se recogen los datos, dónde se guardan, por cuanto tiempo.
- Modo y manera en la que se podrá acceder a la información recogida, y quién podrá acceder a la misma.
- Previsiones de actuación frente a solicitudes del ejercicio de los derechos que la normativa de protección de datos reconoce a los trabajadores, en su condición de titulares de los mismos.
- Pautas de actuación en el caso de que un trabajador cause baja en la empresa.
- Plazo durante el cual estos registros serán conservados.
- Método de supresión de los datos una vez que hayan dejado de ser pertinentes para las finalidades que fueron recogidos.

9. VERIFICACIÓN PERIÓDICA INTEGRIDAD DEL SISTEMA.

Con el fin de mantener un control constante de los sistemas de protección de datos adoptados por la empresa , con carácter periódico y cada vez que se realicen cambios en las actividades de tratamiento la empresa debe realizar auditorías internas de verificaciónperiódicas , donde se analicen todos los puntos de control relacionados con las actividades de tratamiento llevadas a cabo.

Los resultados serán documentados y puestos a disposición de la AEPD y los interesados que así lo soliciten como prueba de conformidad.

PREGUNTAS FRECUENTES

1. ¿Puede un trabajador negarse a firmar el documento que le informa del nuevo tratamiento de sus datos y de su finalidad?

Es a la empresa al que le corresponde la carga de probar que ha informado debidamente a sus trabajadores del nuevo tratamiento de sus datos. La negativa de un trabajador no tiene mayores consecuencias para la empresa,

siempre que acredite por otros medios que puso a su disposición la información legalmente exigida, como la firma de testigos.

2. ¿Durante cuanto tiempo se deben conservar los registros derivados del control de la jornada laboral?

4 años, en virtud de lo dispuesto en el Real Decreto-ley 8/2019, de 8 de marzo

3.- ¿Quién tiene acceso a los registros de control de la jornada laboral?

Según el Real Decreto-ley 8/2019, de 8 de marzo, los trabajadores en cualquier momento, los representantes de los trabajadores y la autoridad laboral, a los que habrá que añadir la inspección de la Agencia Española de Protección de Datos.

Lo anterior no implica la obligación de entrega de copias, salvo pacto expreso en contrario, ni debe entregarse al trabajador copia individualizada de su registro diario, sin perjuicio de facilitar su consulta personal.

4. ¿Debo entregar copia si la representación de los trabajadores la solicitan?

No. Se les podrá dar acceso mostrándoles los registros, pudiendo tomar las notas que consideren necesarias.

5.- ¿Se le aplica esta normativa al Director General?

Salvo que el Director General de la empresa tenga un contrato de alta direcciónde los regulados en el Real Decreto 1382/1985se le deberá registrar el horario.

6.- ¿Y a los mandos intermedios?

No les resultará de aplicación en el caso de que tengan pactado, expresamente, un régimen de libre disponibilidad horaria.

7.- ¿A qué tipo de trabajadores, sectores profesionales y empresas se aplica elregistro horario?

El registro horario se aplica a la totalidad de trabajadores, al margen de su categoría o grupo profesional, a todos los sectores de actividad y a todas las

empresas, cualquiera que sea su tamaño u organización del trabajo, siempre y cuando estén incluidas en el ámbito de aplicación que define el artículo 1 del Estatuto de los Trabajadores.

8.- Soy un trabajador autónomo ¿Me afecta esta Ley?

No

9.- Soy un trabajador autónomo que tiene empleados ¿Me afecta esta Ley?

Sí, en este caso, y respecto de los empleados se deberá llevar a cabo el registro de la jornada laboral.

10.- Soy un trabajador autónomo societario ¿Me afecta esta Ley?

No.

11.- Soy socio de una cooperativa ¿me afecta esta Ley?

Conforme a la Ley 27/1999, de 16 de julio, de ámbito estatal, la relación de los socios con la cooperativa es societaria, por lo que quedan excluidos de la normativa laboral.

12.- ¿Exige la Ley una forma concreta de registrar la jornada laboral?

No. Los únicos requisitos que se exigen enla norma es que el registro de jornada tanto si se realiza en soporte papel como electrónico el sistema debe permitairla trazabilidad de las jornadas diarias y que no sean manipulables a posteriori, ni por el trabajador ni por el empresario.

13.- He descargado un modelo en hoja Excel, ¿cumple este modelo de registro la norma?

Sólo en el caso de que se imprima y se cumplimente una vez impreso en papel, de forma que quede constancia del registro diario, firmado por el trabajador, sin que pueda manipularse posteriormente.

La llevanza del registro horario directamente a través de una hoja Excel en el ordenador no permite acreditar que el registro no ha sido manipulado con posterioridad.

14.- ¿Es el Delegado de Protección de Datos (DPO) el encargado del análisis de riesgos?

Sí, en las empresas que hayan designado un **DPO,** esta será la persona responsable de llevar a cabo el análisis de riesgos y de determinar si una **Evaluación de Impacto en Protección de datos (EIPD)** es necesaria.

No obstante, puesto que no todas las empresas requieren de la designación obligatoria de un DPO, las empresas que carecen de esta figura deberán escoger a una persona con las competencias necesarias para llevar a cabo el análisis de riesgos y, en su caso, una evaluación de impacto.

15.- ¿La publicación de esta Ley me exige nombrar un delegado de protección de datos?

Disponer de un profesional cualificado en una materia tan específica y compleja como la protección de datos siempre es recomendable aunque no exista obligación legal de nombrarlo.

No obstante, esta norma no exige disponer de esta figura a salvo de los casos ya previstos en la ley.

16.- El servicio externo que he seleccionado implica también como funcionalidad la geolocalización de los trabajadores, ¿en qué medida me afecta?

La geolocalización implica, por imperativo legal, un tratamiento de datos especialmente invasivo de la intimidad de las personas, por lo que todo lo dicho en esta guía para el tratamiento de datos biométricos, análisis de riesgos y evaluación de impacto en protección de datos así como el deber de informar al trabajador, entre otras cuestiones, deberán hacerse de manera independiente al del tratamiento biométrico, pues supone un tratamiento de datos de distinta naturaleza.

17.- ¿Sirve cualquier dispositivo y software para controlar, mediante huella dactilar, la jornada laboral?

La Agencia Española de Protección de Datos considera que los sistemas menos invasivo para registrar la huella dactilar, y por tanto, que cumple con los principios de proporcionalidad y minimización son aquellos en los que los datos biométricos se incorporasen a una tarjeta inteligente que quedara en poder del usuario.

De ese modo para acceder a las instalaciones utilizaría la tarjeta y posicionaría su huella sobre el lector. El sistema informático central no almacenaría el algoritmo que estaría en la tarjeta personal.

Sin embargo, esto no es obstáculo para usar otro tipo de dispositivos y software que puedan ser capaces de pasar con éxito el análisis de riesgos y la evaluación de impacto en protección de datos.

18.-¿Se puede eliminar con este nuevo registro el de las horas extraordinarias que estábamos llevando hasta el momento?

El registro diario de jornada y el registro de horas extraordinarias son obligaciones legales independientes pero compatibles. No obstante, si el mismo sistema permite registrar ambas obligaciones, entonces sí es posible integrar ambas obligaciones en un solo sistema.

19.- ¿Se puede sancionar a los trabajadores si se olvidan o no registran correctamente sus jornadas?

Sería necesario que tal sistema sancionador viniera recogido en una política o protocolo de registro de jornada, que el mismo se haya negociado, en su caso con la representación de los trabajadores, y se haya informado convenientemente a los empleados.