Anexos II

ANEXO. 9

INSTRUCCIONES DE LA SUBDELEGADA DE PROTECCIÓN DE DATOS (ENCARGO A MEDIOS PROPIOS PERSONIFICADOS PARA LA ASISTENCIA TÉCNICA DE APOYO A LA ATENCIÓN TELEFÓNICA Y A LA TRAMITACIÓN RELATIVA AL INGRESO MÍNIMO VITAL)

INSTRUCCIONES RESPECTO DE LOS ENCARGOS DE GESTIÓN REALIZADOS POR EL INSTITUTO NACIONAL DE LA SEGUIDAD SOCIAL (INSS) A LA SOCIEDAD ESTATAL TECNOLOGÍAS Y SERVICIOS AGRARIOS (TRAGSATEC), REFERIDOS A LA "ASISTENCIA TÉCNICA DE APOYO A LA CAPTURA Y TRAMITACIÓN DE LA GESTIÓN ELECTRÓNICA DE LAS PRESTACIONES ECONÓMICAS DEL INGRESO MÍNIMO VITAL" (IMV), Y LA "ASISTENCIA TÉCNICA DE APOYO A LA ATENCIÓN E INFORMACIÓN TELEFÓNICA PARA LA NUEVA PRESTACIÓN DEL INGRESO MÍNIMO VITAL".

Mediante Resoluciones de 9 de Junio de 2020, de la Directora General del Instituto Nacional de la Seguridad Social, se ha encargado a TRAGSATEC la asistencia técnica de "*Apoyo en la captura y tramitación de la gestión electrónica de las prestaciones económicas del IMV", y "Asistencia técnica de apoyo a la atención e información telefónica para la nueva prestación del IMV".*

Al efecto de establecer el marco general en el que deben desenvolverse las condiciones técnicas y económicas, TRAGSATEC, conforme a las directrices establecidas por el INSS, deberá llevar a cabo las actividades, de acuerdo con lo dispuesto en el *Anexo I "Programa de actividad"* de cada encargo, en cuyo punto 1 se establecen los objetivos y en el punto 2 se concretizan las actividades a desarrollar.

Por lo que se refiere a la protección de datos personales, la *cláusula Sexta. Protección de datos personales*, de ambos encargos, recoge de forma expresa las distintas obligaciones que asumen el INSS (como Responsable) y TRAGSATEC (como Encargado) en materia de protección de datos, respecto del tratamiento de datos del IMV, así como las derivadas del Deber de confidencialidad.

Debe reseñarse el *Anexo III "Tratamiento de datos personales",* en el que se realiza una descripción general del tratamiento de Datos Personales a efectuar, en ambos encargos, por TRAGSATEC.

Así pues, dentro del poder de dirección que ostenta el INSS en el desarrollo de los encargos de gestión en cuestión, y de forma expresa respecto al tratamiento de datos personales del IMV, se establecen las siguientes directrices de actuación, con la finalidad de complementar el clausulado y anexos de las Resoluciones de 9 de junio de 2020:

1. Procedimiento de actuación ante solicitudes de ejercicio de derechos.

2. Comunicaciones de brechas de seguridad.

3. Confidencialidad y deber de sigilo.

4. Destino de los datos.

1. PROCEDIMIENTO DE ACTUACIÓN ANTE SOLICITUDES DE EJERCICIO DE DERECHOS:

Conforme el art. 28.3 letra e) del Reglamento (UE) 2016/679, General de Protección de Datos (RGPD), el encargado del tratamiento: *"asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III*(derechos en materia de protección de datos)".

Así pues, cuando un ciudadano desee ejercitar alguno de los derechos reconocidos en la normativa de protección de datos ante TRAGSATEC, se le facilitará el modelo correspondiente , a cuyos efectos se podrá utilizar tanto el elaborado por el INSS, como por la Agencia Española de Protección de datos (AEPD) o en su caso el previsto en el Sistema de Gestión de Protección de Datos - Protocolo Tramitación Derechos

PADRE DAMIAN 4
28036 MADRID
TEL.: 91 568 83 00
FAX: 91 561 10 51
Código DIR3: EA0021203

ARCOPO del Grupo empresarial TRAGSA. Una vez cumplimentado se registrará por parte de TRAGSATEC y se enviará a la Dirección Provincial correspondiente, para su tramitación. Esta comunicación deberá hacerse de forma inmediata y en ningún caso más allá del segundo día laborable siguiente al de la recepción de la solicitud, juntamente en su caso, con la documentación y otras informaciones que puedan ser relevantes para resolver la solicitud (datos personales tratados referidos al interesado, unidad de TRAGSATEC que lo ha realizado, lugar y sistemas información y aplicativos informáticos utilizados, destinatarios de los datos, etc.).

Además del modelo oficial, los usuarios **podrán presentar su propia solicitud** siempre que cumpla, como mínimo, **los siguientes requisitos:**

- Nombre y apellidos del interesado
- Fotocopia del DNI, pasaporte, o NIE. También la de la persona que lo representa cuando se actúe en representación. Si la solicitud se realiza por medios telemáticos, se acreditará la identidad a través de la firma electrónica
- Dirección a efectos de notificaciones
- Petición en que se concreta la solicitud
- Fecha y firma

Una vez presentada, **se entregará al interesado una copia sellada** de la solicitud.

Si la solicitud no reúne los requisitos especificados anteriormente, se deberá solicitar la subsanación de estos, fijándose un **plazo de subsanación de 10 días**. De no presentarse en el citado plazo, se considerará como desistida su petición, de conformidad con los artículos 68 y 69 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Cuando la solicitud se refiera a actividades, ficheros o bases de datos personales que no guarden relación con el tratamiento de datos del IMV, se remitirá igualmente al INSS, comunicando al interesado dicha circunstancia y la fecha del traslado.

La Dirección provincial donde se haya presentado la solicitud para el ejercicio de los derechos, **deberá resolver en el plazo de un mes** a contar desde el momento en que se presentó la solicitud ante TRAGSATEC.

En **caso de que surjan dudas sobre cómo se ha tramitar la solicitud**, se deberá recabar el asesoramiento de la Subdelegada de Protección de Datos del INSS a través del **buzón de consultas corporativo**: **consultas.inss-sscc.proteccion-de-datos@seg-social.es**

2. COMUNICACIÓN DE UNA BRECHA DE SEGURIDAD DE LOS DATOS PERSONALES:

Conforme el **Esquema Nacional de Seguridad (ENS)** y la **Directiva NIS**, se define un **"incidente de seguridad"** como aquel evento o serie de eventos, inesperados o no deseados, con consecuencias negativas para la seguridad del sistema de información, y que, con una gran probabilidad, van a comprometer las operaciones de la organización y amenazar la seguridad de la información, teniendo efectos adversos en la seguridad de las redes y sistemas de información.

PADRE DAMIAN 4
28036 MADRID
TEL.: 91 568 83 00
FAX: 91 561 10 51
Código DIR3: EA0021203

No obstante, a efectos de protección de datos, solo resultan de interés aquellos incidentes de seguridad que deban considerarse como una **"brecha de seguridad".**

Un incidente de seguridad constituirá una brecha de seguridad cuando cumpla todas las condiciones siguientes:

1. **Afecte a la seguridad de información,** es decir, ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
2. **Afecte a datos personales.**
3. **Suponga un riesgo** para los derechos y libertades de las personas físicas titulares de los datos.

Las brechas de seguridad pueden producirse tanto en sistemas informáticos (aplicativos informáticos, bases de datos, ficheros informáticos, tabletas, PCs, teléfonos móviles, cds, memorias de almacenamiento, etc.), como en tratamientos en papel (formularios o expedientes en papel, carpetas o archivadores a-z,…).

La normativa vigente impone al Responsable del tratamiento (INSS) la **obligación de notificar a la autoridad de control (AEPD) toda brecha de seguridad** que se haya producido en el ámbito de su competencia, en el **plazo máximo de 72h** desde que haya tenido conocimiento de ello.

Así pues, TRAGSATEC, en su calidad de encargado de tratamiento, deberá notificar al responsable del tratamiento (INSS), sin dilación indebida, las violaciones de seguridad de los datos personales a su cargo de las que tenga conocimiento, junto con toda la información relevante para la documentación y comunicación de la incidencia, conforme el siguiente procedimiento:

1. Informará a la persona responsable en materia de protección de datos de la Dirección provincial de la situación producida.
2. Una vez comunicados los hechos o situación producida, se deberá confirmar que el incidente en cuestión se trata de una brecha de seguridad.
3. De forma simultánea a la comunicación anterior, TRAGSATEC deberá adoptar las medidas necesarias para poner fin a la brecha de seguridad, y para corregir y paliar los efectos nocivos que se hayan podido producir.
4. Todo lo expuesto en los puntos anteriores, se deberá realizar a la mayor brevedad posible, y siempre antes del transcurso de 48 horas desde que se produjo o se tuvo conocimiento de la incidencia, comunicándolo a la Subdelegada de Protección de Datos del INSS a través del buzón de consultas de protección de datos (**consultas.inss-sscc.proteccion-de-datos@seg-social.es**) o al buzón de la Inspección de Servicios (**inspeccion.inss-sscc.sg@seg-social.es**), en ambos casos del INSS.
5. La comunicación expuesta en el punto anterior deberá contener la siguiente información:
    1. Naturaleza de la brecha de seguridad:

PADRE DAMIAN 4
28036 MADRID
TEL.: 91 568 83 00
FAX: 91 561 10 51
Código DIR3: EA0021203

- Brecha de confidencialidad (acceso no autorizado)
- Brecha de integridad (modificación no autorizada)
- Brecha de disponibilidad (desaparición o pérdida)

2. Categorías de afectados:
- Menores o discapacitados.
- Empleados públicos.
- Ciudadanos.

3. Medio por el que se ha materializado la brecha:
- Dispositivo perdido o robado.
- Documentación perdida, robada.
- Correo perdido o abierto.
- Datos personales mostrados al individuo incorrecto.
- Revelación verbal no autorizada de datos personales.
- Eliminación incorrecta de datos personales formato papel.
- Datos personales residuales en dispositivos obsoletos.

4. Nº aproximado de afectados.

5. Categorías de datos comprometidos:
- Identificativos, DNI, NUSS, NIE.
- Credenciales de acceso o identificación.
- Datos de contacto o residencia.
- Datos económicos o financieros.
- Datos de salud.

6. Nº registros de datos personales afectados.

7. Posibles consecuencias de la brecha de seguridad sufrida.

8. Medidas adoptadas o propuestas para remediar la brecha.

9. Si se le ha comunicado la brecha al afectado.

10. Fechas en las que han sucedido todos los hechos.

IMPORTANTE:

Es fundamental que las brechas de seguridad se comuniquen al buzón indicado en el **plazo máximo de 48h**.

Si no se dispone de toda la información, es posible su ampliación con posterioridad, lo urgente es la comunicación inicial.

Las notificaciones a la AEPD solo se realizarán por parte de la Subdelegada de Protección de Datos del INSS, **nunca por TRAGSATEC**.

PADRE DAMIAN 4
28036 MADRID
TEL.: 91 568 83 00
FAX: 91 561 10 51
Código DIR3: EA0021203

3. CONFIDENCIALIDAD Y DEBER DE SIGILO:

TRAGSATEC deberá realizar los trabajos derivados de los encargos de gestión en cuestión, con la única, exclusiva y excluyente finalidad de satisfacer las actividades descritas en los *ANEXO I. Programa de actividad* de las Resoluciones de 9 de junio de 2020.

En todo momento, TRAGSATEC deberá actuar con la máxima diligencia debida respecto de los datos personales que conozca en el desempeño de los encargos, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento del IMV, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas que podrían verse afectadas.

Así mismo, TRAGSATEC deberá guardar la debida confidencialidad respecto a los hechos, datos e informaciones que conozca en el curso de los encargos, aun cuando no se refieran a datos de carácter personal.

Igualmente, se compromete a proteger la documentación e información generada y obtenida (en cualquier formato) a la que tenga acceso su personal autorizado con motivo de la ejecución de las actividades encargadas, con las medidas, procedimientos y medios adecuados para garantizar la confidencialidad, integridad, disponibilidad de la información manejada, así como la trazabilidad de las acciones realizadas por su personal en el desarrollo de su trabajo conforme a la normativa vigente de general aplicación.

TRAGSATEC establecerá las medidas, procedimientos y medios de seguridad necesarios y adecuados para impedir la utilización de la información en provecho de terceras personas, fundamentalmente en el caso de tratamiento de datos personales sensibles especialmente protegidos por las normas vigentes en materia de protección de datos personales expresamente relacionadas en los encargos efectuados.

En todo momento, el INSS, como responsable del tratamiento, podrá exigir y realizar las auditorías que estime oportunas para supervisar y comprobar que los accesos o actuaciones realizadas sobre los aplicativos, herramientas o sistemas informáticos puestos a disposición de TRAGSATEC, se han llevado a cabo exclusivamente con ocasión del desempeño de los encargos de gestión, pudiendo comprobar los datos identificativos del trabajador, hora y actuación realizada y finalidad por la que lo hizo, entre otros extremos.

No obstante, TRAGSATEC podrá establecer cuantas medidas de seguridad, técnicas y organizativas estime oportunas con el fin de garantizar la disponibilidad, integridad, confidencialidad, acceso y trazabilidad de la información aportada por los solicitantes de la prestación del IMV. Siempre informando de todo ello al INSS, y suministrando los resultados y documentación que acrediten dichas medidas de seguridad.

4. DESTINO DE LOS DATOS:

Todos los datos personales que se traten o elaboren por TRAGSATEC como consecuencia de los encargos de gestión, así como los soportes del tipo que sean en los que se contengan son propiedad del INSS**.**

PADRE DAMIAN 4
28036 MADRID
TEL.: 91 568 83 00
FAX: 91 561 10 51
Código DIR3: EA0021203

En la medida que el encargado aporta equipos informáticos para la prestación del servicio objeto de los encargos, una vez finalizadas las tareas, el encargado, previamente a retirar los equipos informáticos, deberá borrar toda la información utilizada o que se derive de la ejecución de los encargos mediante el procedimiento técnico adecuado o proceder a su entrega al responsable del tratamiento.

Así, deberá procederse a la destrucción de la documentación de apoyo (por ejemplo, las anotaciones que en soporte papel se efectúen por el personal contratado por TRAGSATEC, esquemas, etc.), si no se considerara indispensable por el INSS, habiéndolo comunicado por escrito. La destrucción se efectuará mediante máquina destructora de papel o cualquier otro medio que garantice la ilegibilidad, llevándose a cabo esta operación en el lugar donde se realicen los trabajos. Igualmente, deberá adoptar las medidas necesarias para impedir la recuperación posterior de información almacenada en soportes que vayan a ser desechados o reutilizados.

Se deberá devolver al responsable del tratamiento (INSS) los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación.

La devolución debe comportar el borrado total de datos existentes en los equipos informáticos utilizados en cada uno de los encargos.

LA SECRETARIA GENERAL Y

SUBDELEGADA DE PROTECICÓN DE DATOS

ANA MARIA FEIJOO ALONSO - 34960679N

Firmado digitalmente por ANA MARIA FEIJOO ALONSO - 34960679N
Fecha: 2020.07.07 14:03:41 +02'00'

PADRE DAMIAN 4
28036 MADRID
TEL.: 91 568 83 00
FAX: 91 561 10 51
Código DIR3: EA0021203

ANEXO. 10

DEBER DE INFORMACIÓN: VISITAS DE INSPECCIÓN ONLINE

Asunto: INSPECCIONES A REALIZAR TRAVES DE PLATAFOMA TEAMS

Estimado director/a

Una de las competencias de la Secretaría General es la inspección y supervisión de la actuación y funcionamiento de las distintas unidades de la Entidad.

El ejercicio de esta función ha evolucionado con el tiempo, de la mano de los cambios funcionales y tecnológicos, y de un cambio de " filosofía", inspirada, no solo en la identificación de disfunciones en los distintos espacios de análisis y actuación, sino también, y muy fundamentalmente, en la gestión del conocimiento mediante la difusión entre las Direcciones Provinciales de las buenas prácticas identificadas en las inspecciones realizadas.

La situación sanitaria creada por la Covid 19 obliga a llevar a cabo una nueva adaptación, en este caso, del formato, a través del cual contactar con las Direcciones provinciales objeto de inspección. En efecto, la instrucción novena de la Resolución del Secretario de Estado de Política Territorial y Función Pública, de fecha 17 de junio de 2020, que determina las medidas a adoptar en los centros de trabajo dependientes de la administración general del estado con motivo de la nueva normalidad, establece lo siguiente:

"Novena.- Viajes.
Se suspenderán todos aquellos viajes de trabajo que puedan solventarse mediante llamada o videoconferencia."

Por ello, te anticipo las características de acuerdo con las que se llevarán a cabo las inspecciones, en adelante.

A partir del mes de septiembre las inspecciones se realizarán a distancia, a través de Microsoft Teams.

Microsoft Teams es una herramienta que permite:

- ü Iniciar reuniones de vídeo o voz. Durante estas reuniones o conferencias se puede compartir escritorio y una pizarra virtual.
- ü Realizar chats individuales o de grupo. Se trata de mensajes instantáneos en Skype Empresarial, como los de cualquier otra aplicación de mensajería. El contenido y el historial de chat se puede consultar en cualquier momento. Los chats sólo son visibles para las personas con las que se realiza el chat (un usuario y otra persona o un grupo de personas).
- ü Disponer de un espacio común de trabajo con interfaz web y aplicación para PC, así como una aplicación para dispositivos móviles.

Para la realización de las inspecciones se seguirán los siguientes pasos:

1. Comunicación por la Jefa de la Inspección, al Director Provincial, del programa de inspección que se va a realizar y del inspector designado al efecto.
2. Comunicación por el director provincial, en la jornada siguiente, del interlocutor con el que el inspector despachará los asuntos necesarios para llevar a cabo la inspección, y de los funcionarios implicados en la realización de la misma (secretario provincial, subdirectores provinciales, jefes de sección, coordinadores de CAISS, tramitadores, en su caso…), a fin de que por el inspector se programen las entrevistas.
3. Comunicación del inspector, dirigida al interlocutor designado, para solicitar la documentación necesaria para la inspección. Toda la documentación que la Dirección Provincial deba poner a disposición del inspector deberá situarse en una carpeta informática determinada a la que se permita el acceso al inspector.

4. Análisis de la documentación y establecimiento, de un calendario de acuerdo con la Dirección Provincial, de los días y las horas para realizar las entrevistas con las personas afectadas. Desde la Inspección de Servicios se enviará una invitación para llevar a cabo la entrevista a través de Microsoft Teams, en el día y hora determinados.

Para la realización de las reuniones de trabajo y entrevistas será preciso que la Dirección Provincial disponga de un ordenador con cámara y auriculares.

AVISO SOBRE PROTECCIÓN DE DATOS PERSONALES:

De conformidad con lo dispuesto en el artículo 13 del Reglamento (UE) 2016/679 General de Protección de Datos Personales y el artículo 11 de la ley Orgánica 3/2018, de Protección de Datos personales y garantía de los derechos digitales, se informa que mediante las entrevistas a realizar por videoconferencia o de forma telefónica durante el curso de la inspección, se podrán obtener y recopilar los datos personales suministrados por el funcionario que participe en la misma, para su posterior uso por parte de la Inspección de Servicios, unidad adscrita a la Secretaría General del INSS, responsable del tratamiento, con la finalidad de desempeñar sus funciones de control, vigilancia y supervisión de los servicios y actividades desempeñadas por la dirección provincial.

En ningún caso serán objeto de tratamiento los datos personales referidos a la imagen o voz del funcionario, quedando prohibida de forma expresa su grabación. Igualmente, queda prohibida la grabación de la imagen o voz del inspector que venga realizando la actividad inspectora

Puede ejercer sus derechos en materia de Protección de Datos en cualquier momento. Para más información consulte la web: www.seg-social.es (apartado de protección de datos).

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS
NOMBRE DEL TRATAMIENTO
Procesos internos de Inspección
FINES DEL TRATAMIENTO
Funciones de control, vigilancia y supervisión de los servicios y actividades desempeñadas por la dirección provincial y sus empleados públicos.
RESPONSABLE DEL TRATAMIENTO
Secretaría General del Instituto Nacional de la Seguridad Social
EJERCICIO DE DERECHOS
Se podrán ejercer, cuando procedan, los derechos reconocidos en los arts. 15 a 22 del Reglamento (UE) 2016/679, General de Protección de Datos, mediante un escrito dirigido al responsable del tratamiento, la Delegada de Protección de Datos, o en su caso, la Agencia Española de Protección de Datos.
BASE JURÍDICA - LEGITIMACIÓN
-Reglamento (UE) 2016/679, General de Protección de Datos: Art.6.1.c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable. Art. 6.1.e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable. -Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social. -Real Decreto 799/2005, de 1 de julio, por el que se regulan las inspecciones generales de servicios de los departamentos ministeriales. -Real Decreto 2583/1996, de 13 de diciembre, de estructura orgánica y funciones del Instituto Nacional de la Seguridad Social y de modificación parcial de la Tesorería General de la Seguridad Social.
DATOS DE CONTACTO DEL RESPONSABLE
consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO DE PROTECCIÓN DE DATOS
delegado.protecciondatos@seg-social.es
Para mas información consulte el apartado de protección de datos de la web o de la sede electrónica de la seguridad social: www.seg-social.es

ANEXO. 11

GUÍA DE PROTECCIÓN DE DATOS PERSONALES EN EL INSS

GUÍA DE PROTECCIÓN DE DATOS

INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL

INDICE

1. PRESENTACIÓN

En el año 2016, la Unión Europea aprobó el Reglamento (UE) 2016/679, General de Protección de Datos (RGPD) que, si bien entró en vigor en mayo de ese año, es de aplicación desde el 25 de mayo de 2018. Al tratarse de un Reglamento europeo, no necesita transposición al ordenamiento jurídico español, por lo que su **contenido es directamente aplicable.**

Es decir, esta norma europea, desplazó de forma tácita a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, norma interna sobre protección de datos que quedó derogada de forma expresa por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales (LOPDGDD), la cual ha introducido una serie de cambios en los tratamientos de datos personales que realizan los responsables, así como los denominados encargados. En cuanto al Reglamento de desarrollo de la LO 15/1999, este continúa vigente en lo que no contradiga al RGPD y la LOPDGDD.

NORMATIVA BÁSICA EN MATERIA DE PROTECCIÓN DATOS PERSONALES

- Reglamento (UE) 2016/679, General de Protección de Datos (RGPD)
- LO 3/2018, de Protección de Datos y garantía de los derechos digitales (LOPDGDD)
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de protección de datos de carácter personal.

Así, se introducen, entre otras, las siguientes novedades:

- El principio de responsabilidad activa,
- El principio de minimización de datos personales,
- La figura del Delegado de Protección de Datos,
- La Privacidad desde el Diseño,
- La Privacidad por Defecto,
- Las notificaciones de quiebras de seguridad que puedan afectar a los datos personales, y
- Las Evaluaciones de impacto en la protección de datos.

Otra de las novedades ha consistido en la supresión de la inscripción obligatoria de ficheros, si bien, los responsables y encargados de tratamientos deben configurar el denominado Registro de Actividades de Tratamiento, así como el contenido del derecho de información en la recogida de datos que debe facilitarse a los afectados, puesto que se amplía considerablemente. Resultado de ello es la confluencia de los más de 1300 ficheros de datos personales existentes en el conjunto de las 52 direcciones provinciales y los servicios centrales, en los actuales 43 tratamientos de datos en los que han sido aglutinados, y cuya consulta es accesible desde la web de la Seguridad Social (**www.seg-social.es**)

Dentro de este nuevo marco normativo, el Instituto Nacional de la Seguridad Social (INSS) está comprometido con el respeto a la privacidad del usuario. Para ello, cuenta

con todos los medios técnicos a su alcance y la permanente colaboración de la Gerencia de Informática de la Seguridad Social (GISS), a fin de garantizar una seguridad adecuada de los datos personales, evitando la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos facilitados a dicho organismo.

Los empleados así como los beneficiarios del Sistema de Seguridad Social deben tener conocimiento de las normas, las salvaguardias y los derechos relativos al tratamiento de sus datos personales así como del modo de hacer valer sus derechos en relación a dicho tratamiento. Es por ello, por lo que se ha procedido a la actualización de la información a suministrar a los afectados en el conjunto de formularios, y procedimientos competencia de esta entidad, en los que se produce una recogida y/o uso de sus datos personales.

En consecuencia, en esta Guía se analizan los aspectos más relevantes del RGPD y la LOPDGDD en relación con los tratamientos de datos personales por parte del INSS.

2. CONCEPTOS Y DEFINICIONES

En la actual sociedad de la información en la que vivimos, cada día se tratan millones de datos personales. Sin el uso de nuestra información personal, prácticamente ninguno de los servicios de los que disponemos podría funcionar, imposibilitando el ejercicio de las funciones que tiene atribuidas el INSS. Así pues, es conveniente definir los siguientes conceptos, fundamentales en materia de protección de datos:

- **Dato personal:** toda información sobre una persona física identificable (directa o indirectamente). Se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

- **Tratamiento:** cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

- **Fichero:** todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

- **Responsable del tratamiento:** la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o

los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

- **Encargado del tratamiento:** la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. Por ejemplo, los servicios de videovigilancia, los que realizan reconocimientos médicos de los empleados o los que llevan a cabo el expurgo de la documentación

- **Destinatario:** la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

- **Tercero:** persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

- **Empresa:** persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica. A efectos de protección de datos personales, **los trabajadores autónomos** tienen la consideración de empresa, y por lo tanto de persona jurídica y no persona física, no siéndole aplicable la normativa en cuestión.

- **Consentimiento del interesado:** toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

- **Datos biométricos:** 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 dicha persona, como imágenes faciales o datos dactiloscópicos.

- **Datos relativos a la salud:** datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud. La existencia de una discapacidad, el grado reconocido, así como de una pensión de incapacidad y su tipo, son datos que revelan un dato de salud de las personas afectadas.

- **Elaboración de perfiles:** toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

- **Seudonimización:** el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable

- **Autoridad de control:** la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51 del RGPD, es decir, la Agencia Española de Protección de Datos (AEPD), o en su caso, organismo de carácter autonómico similar.

- **Violación de la seguridad de los datos personales:** toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Por ejemplo: la pérdida de un pendrive, de un cd, un ordenador portátil o una tablet, o de documentación en la basura o en la cafetería…

EJEMPLOS DE CATEGORÍAS DE DATOS PERSONALES OBJETO DE TRATAMIENTO POR EL INSS:

- **La imagen personal y el sonido de la voz (videovigilancia, grabaciones alocuciones telefónicas).**

- **De carácter identificativo (nombre, apellidos, teléfono, correo electrónico, DNI/NIF, NUSS, firma manuscrita).**

1. DATOS PERSONALES

1.1 DEL FUTURO TITULAR DE LA PENSIÓN

Primer apellido	Segundo apellido	Nombre

Fecha de nacimiento	Sexo	Estado civil actual	Está incapacitado judicialmente	Nombre de:	DNI - NIE - Pasaporte
Día ..... Mes ..... Año	Hombre ☐ Mujer ☐	Soltero/a ☐ Casado/a ☐ Viudo/a ☐ Separado/a legalmente ☐ Divorciado/a ☐	SÍ ☐ NO ☐ Tiene reconocida discapacidad SÍ ☐ NO ☐	Padre ..... Madre	Nº de la Seguridad Social / Nacionalidad / Teléfono fijo

Domicilio habitual: (calle, plaza …)	Número	Bloque	Escalera	Piso	Puerta	Teléfono móvil

Código postal	Localidad	Provincia	País

- **De carácter tributario (IRPF, tipo deducciones).**

4.4 DATOS DEL FUTURO TITULAR A EFECTOS FISCALES

Residencia fiscal: Provincia ..... País .....

Si está en territorio común y desea un tipo voluntario de retención por IRPF indique cuál: ... . %

Tiene reconocida discapacidad ... de 33% a 64% ☐ más de 64% ☐

Ayuda de 3ª persona o movilidad reducida ... SÍ ☐ NO ☐

Cuantía anual de pensión compensatoria ... . €

Cuantía anual de alimentos a favor de los hijos: ... . €

Si está pagando préstamos por adquisición o rehabilitación de su vivienda habitual desde antes del 01/01/2013 y sus rendimientos de trabajo anuales, incluida ésta y otras pensiones, son inferiores a 33.007,20 €, marque este recuadro ... ☐

Si está en TERRITORIO FORAL, a efectos de retención por IRPF desea que se le aplique:

Tabla general ☐ Nº de hijos .....

Tabla de pensionistas ☐

Tipo voluntario: ☐ ..... %

- **De carácter financiero (nº cuenta bancaria, nº tarjeta bancaria).**

8. COBRO DE LA PENSIÓN

PAGO EN ESPAÑA (Banco o Caja de Ahorro)

BIC: .....

En cuenta del: Futuro titular de la pensión (1.1) ☐ Tutor (1.2) ☐

Código IBAN (antigua cuenta corriente)	CÓDIGO PAÍS	CCC			
		ENTIDAD	OFICINA/ SUCURSAL	DÍG. CONTROL	NÚMERO DE CUENTA

PAGO EN EL EXTRANJERO Cheque ☐ Transferencia ☐ País .....

BIC: ..... IBAN: ..... CCC: .....

- **Categorías especiales de datos (origen racial, etnia, datos de salud u orientación sexual).**

1.1	PROGENITOR SOLICITANTE								
Primer apellido		Segundo apellido		Nombre JUAN FRANCISCO					
Fecha de nacimiento	Sexo ☑ Hombre ☐ Mujer	DNI-NIE-Pasaporte	Nº de la Seguridad Social		Nacionalidad				
Domicilio (calle, plaza ...)			Número	Bloque	Escalera	Piso	Puerta	Teléfono móvil	
Código postal	Localidad	Provincia	Correo electrónico						

1.2	DATOS INDENTIFICATIVOS DEL OTRO PROGENITOR		
Primer apellido	Segundo apellido	Nombre MANUEL ALBERTO	
DNI-NIE-Pasaporte	Nº de la Seguridad Social		

- **Académicos y profesionales (títulos universitarios, académicos, certificados, experiencia profesional, etc.).**

PUESTOS DESEMPEÑADOS COMO PERSONAL FUNCIONARIO DE CARRERA Y SITUACIONES ADMINISTRATIVAS [Base Tercera A)] en los **últimos 1.826 días naturales** (inmediatamente anteriores a la fecha de finalización del plazo de presentación de solicitudes): figurarán todos los puestos, relacionados de menor a mayor antigüedad; para los casos de excedencia voluntaria por cuidado de hijo o familiar (art. 89.4 del EBEP) y servicios especiales indicar lo expresado en el apartado 7 de la Base Primera. Se reflejarán aquí todos los días, teniendo en cuenta las Consideraciones Generales de la Base Tercera, apartado A). Alternativamente, se hará constar alguna de las situaciones contempladas en la misma Base Tercera A):

	Puesto de trabajo desempeñado	N.C.D.	Días de desempeño en dicho puesto o en la situación administrativa (1)			Código Organismo (Anexo VI)	*(En su caso)* Código Área Funcional (Anexo VII)
			Fecha inicio --/--/--	Fecha finalización --/--/--	Nº total de días		
A)							
B)							
C)							
D)							
E)							
F)							
G)							
...							

(1): La suma de los días completos de desempeño que figuran en las líneas [A), B), C), D), E), F), G)...] nunca podrá ser superior a 1.826 días.

CURSOS REALIZADOS (de carácter administrativo, informático, protección de datos, procedimiento administrativo), según Base Tercera, B), 1.3

Literal del curso	Centro que lo impartió	Año	Horas:

2.1. ¿QUÉ ES UN TRATAMIENTO DE DATOS PERSONALES?

Cualquier actividad en la que estén presentes datos personales constituye un tratamiento de datos, ya se realice de manera manual o automatizada, total o parcialmente:

- La recogida y registro,
- La organización, estructuración y conservación,
- La adaptación, modificación o extracción,
- La consulta y utilización,
- La comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, o interconexión,
- La limitación, y
- La supresión o destrucción.

El INSS, de conformidad con la normativa en materia de seguridad social, presta una serie de servicios públicos ligados a las diferentes competencias o funciones que tiene atribuidas. Servicios por los cuales, recaba y utiliza los datos personales de los ciudadanos, que son tratados de forma manual o, total o parcialmente automatizada.

Asimismo, para identificar los tratamientos del INSS se han tenido presentes las competencias del mismo en función de las prestaciones concretas cuya gestión le corresponde.

2.2. ¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES?

El responsable del tratamiento o responsable, es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento.

En el ámbito del INSS, el responsable del tratamiento, considerando la normativa de régimen, estructura y funciones del mismo, es la propia entidad, pudiéndose observar una responsabilidad funcional respecto de los distintos tratamientos atendiendo a la finalidad de los mismos y que recae en las Subdirecciones generales y Direcciones provinciales competentes en razón de la prestación objeto del tratamiento y el ámbito territorial en el que se desarrollan.

EJEMPLOS DE TRATAMIENTOS POR EL INSS:	
Jubilación	**Incapacidad Permanente**
Asistencia Sanitaria	**Incapacidad Temporal**
Videovigilancia y Seguridad	**Recursos Humanos**

2.3. ¿QUIÉN ES EL ENCARGADO DEL TRATAMIENTO?

Es la persona física o jurídica, pública o privada, autoridad pública, servicio u otro organismo que trate datos por cuenta del responsable del tratamiento.

Por ejemplo, cuando una Dirección provincial encarga a un tercero (una empresa):

- El reconocimiento médico de los empleados públicos
- Las traducciones de la documentación en lengua distinta al castellano
- El servicio de videovigilancia y seguridad
- La realización de pruebas médicas a petición de las Unidades Médicas
- La destrucción de la documentación en soporte físico

El INSS, como responsable del tratamiento, debe elegir un encargado del tratamiento que ofrezca garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD y la LOPDGDD, y que garantice la protección de los derechos de las personas afectadas. Existe, por tanto, un **deber de diligencia en la elección del responsable**.

¿Qué significa esto? que el encargado del tratamiento debe ofrecer suficientes garantías en lo referente a conocimientos especializados, fiabilidad y recursos materiales y humanos, con vistas a la aplicación de medidas técnicas y organizativas que cumplan los requisitos de la normativa de protección de datos, incluida la seguridad del tratamiento.

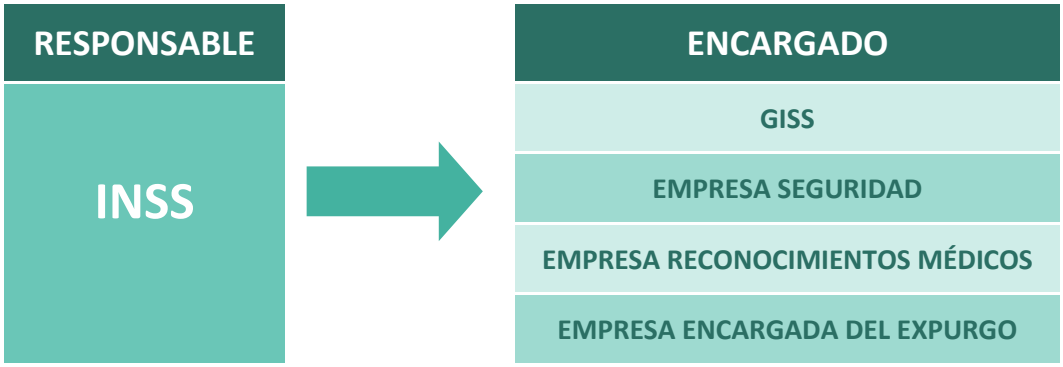
La relación entre el responsable (INSS) y el encargado (empresa) debe estar regulada en un contrato o instrumento jurídico que garantice el compromiso y cumplimiento de las medidas de seguridad y organizativas necesarias para asegurar la confidencialidad, integridad y disponibilidad de los datos personales.

El contenido mínimo de ese contrato o negocio jurídico viene constituido por:

- **Las instrucciones del responsable del tratamiento.**
- **El objeto del encargo.**
- **La duración del mismo.**
- **Finalidad del tratamiento.**
- **Tipo de datos personales que se utilizarán.**
- **Categorías de afectados.**
- **Obligaciones y derechos del responsable.**
- **El deber de confidencialidad.**
- **Las medidas de seguridad a aplicar por el encargado.**
- **El régimen de la subcontratación, en su caso.**
- **La forma en que el encargado asistirá al responsable en el cumplimiento de responder el ejercicio de los derechos de los afectados.**
- **El destino de los datos al finalizar la prestación.**

IMPORTANTE: Todo tratamiento de datos personales que se realice en el ámbito de una Dirección provincial a través de un encargado externo al INSS, debe contar con un contrato que garantice el cumplimiento de la normativa de protección de datos.

En el uso de aplicativos y herramientas informáticas utilizadas para la práctica ordinaria de la actividad gestora del INSS, la Gerencia de Informática de la Seguridad Social (GISS) tiene la consideración de encargada del tratamiento.



2.4. ¿CUÁLES SON LOS PRINCIPIOS APLICABLES AL TRATAMIENTO?

El *RGPD* regula en sus artículos 5 a 11 los principios que deben cumplirse y respetarse cuando se realiza el tratamiento de datos personales de los afectados. Dentro de estos principios podemos distinguir los siguientes:

- Los comprendidos en el artículo 5:
  - **Licitud, Lealtad y Transparencia**
  - **Limitación de la Finalidad**
  - **Minimización de Datos**
  - **Exactitud**
  - **Limitación del Plazo de Conservación**
  - **Integridad y Seguridad**
  - **Responsabilidad Proactiva**
- La licitud del tratamiento (supuestos que legitiman el tratamiento de los datos personales).
- Las condiciones para obtener el consentimiento, incluyendo lo referente al consentimiento de los menores.
- Las condiciones para tratar las categorías especiales de datos personales y para tratar los relativos a condenas e infracciones penales.

Por tanto, estos principios deben cumplirse por el INSS cuando realice el tratamiento de datos de carácter personal de los afectados.

LICITUD, LEALTAD Y TRANSPARENCIA

Los datos personales serán tratados de manera lícita, leal y transparente en relación con el afectado. De esta forma, el tratamiento de los datos personales debe estar amparado en alguna de las bases jurídicas que regula el RGPD, y se excluye que los datos personales sean tratados de forma desleal o sin proporcionar toda la información necesaria sobre el objeto y fines de tratamiento, sus consecuencias y posibles riesgos,

obligando a los responsables que traten los datos personales a ofrecer la mayor transparencia posible sobre el citado tratamiento.

LIMITACIÓN DE LA FINALIDAD

Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados de manera incompatible con dichos fines. No se considerará incompatible con los fines iniciales el tratamiento posterior de los datos con fines de archivo de interés público, fines de investigación científica e histórica o fines estadísticos.

De conformidad con este principio, la finalidad del tratamiento de los datos personales ha de estar claramente definida, así como permitida por el ordenamiento jurídico.

MINIMIZACIÓN DE DATOS

Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No es posible, según este principio, recabar y tratar datos simplemente por si pudieran resultar útiles o “por tenerlos”.

EXACTITUD

Los datos personales serán exactos y si fuera necesario actualizados, adoptándose medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos a los fines para los que se tratan.

IMPORTANTE: Cuando se tenga constancia fidedigna de que un dato personal grabado en un fichero, base de datos o aplicativo del INSS es erróneo, deberá procederse de oficio a su corrección. **Presta especial importancia a los datos del domicilio, nº de identificación personal, nº de cuenta bancaria, etc**. **SIEMPRE ACTUALIZADOS**

LIMITACIÓN PLAZO DE CONSERVACIÓN

Los datos personales serán mantenidos de forma que se permita la identificación de los interesados por un plazo de tiempo no superior al necesario para cumplir con los fines del tratamiento. La conservación de datos debe limitarse a las finalidades para las cuales se han recabado dichos datos. Una vez cumplidas estas finalidades, los datos deben ser borrados o, al menos, desprovistos de todo elemento que permita identificar a los interesados.

Podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo de interés público, fines de investigación científica e histórica o fines estadísticos, sin perjuicio de la aplicación de las correspondientes medidas técnicas y organizativas apropiadas que impone el RGPD.

En el ámbito del INSS, dada la repercusión que dichos datos pueden tener en terceras personas ajenas a los titulares de dichos datos, así como su obligatoria integración en el archivo de la Administración General del Estado, dicho principio será de **aplicación restrictiva y excepcional**. Es por ello, por lo que en la mayoría de los tratamientos existirá la **obligación legal de conservarlos**.

INTEGRIDAD Y SEGURIDAD

Los datos personales serán tratados de manera que se garantice su adecuada seguridad, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, aplicando las medidas técnicas y de organización apropiadas. De acuerdo a este principio, los empleados que traten datos personales deben actuar proactivamente con el objetivo de protegerlos frente a cualquier riesgo que amenace su seguridad, exigiéndoseles la diligencia debida en razón de sus funciones y cargo.

RESPONSABILIDAD PROACTIVA

Los responsables y encargados de tratamiento deben cumplir estos principios y ser capaces de demostrar dicho cumplimiento. El RGPD establece un catálogo de medidas que ambos deben aplicar para garantizar que los tratamientos de los datos son conformes con ambas normas.

Piensa siempre en términos de seguridad, pregúntate qué datos son necesarios para el trámite administrativo que estás realizando, adopta las medidas necesarias para garantizar la integridad, disponibilidad y confidencialidad de los datos.

IMPORTANTE: ya sea en un registro o en un correo electrónico, **restringe la información que expones en el asunto** a la estrictamente necesaria para su identificación

3. ADECUACIÓN DEL INSS A LA NUEVA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES

Con la entrada en vigor de la nueva normativa en materia de protección de datos personales (RGPD y LOPDGDD), el INSS se ha visto obligado a realizar una serie de actuaciones destinadas a adaptar el uso da los datos personales que realiza en sus diferentes tratamientos. Todo ello como consecuencia del Principio de Responsabilidad Proactiva, para así poder asegurar el cumplimiento de la normativa en dicha materia, así como poder demostrar su cumplimiento con evidencias su cumplimiento.

Del catálogo de actuaciones que se han realizado por parte de nuestra Entidad, destacan cuatro:

1. Inclusión y adaptación de la información a suministrar a los ciudadanos en materia de protección de datos en los distintos trámites y procedimientos en los que se recopila sus datos personales;
2. Convergencia y transformación de los antiguos ficheros SIGLA inscritos en el Registro de la AEPD, en los actuales Tratamientos de Datos Personales, inventariados en el Registro de Actividades de Tratamientos publicado por el INSS;
3. Instauración de la figura del Delegado de Protección de Datos y creación de una estructura organizativa de apoyo al mismo en el ejercicio de sus funciones;
4. Actualización y ampliación del apartado específico sobre Protección de Datos Personales en la intranet del INSS y de la Seguridad Social;

A continuación se desglosa este catálogo de medidas que inciden en el mencionado principio de responsabilidad proactiva, y que además, puede tomarse en cuenta como *"hoja de ruta"* para comprender la adaptación de los sistemas de información del INSS a la nueva normativa.

3.1. IDENTIFICACIÓN DE LA LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

Ante el diseño o implementación de un tratamiento de datos personales, lo primero que debe analizarse es si se tiene habilitación legal para obtener y utilizar los datos personales que van a ser objeto de ese tratamiento en relación con la finalidad perseguida por el mismo, es decir, se trata de observar si el INSS al recabar y utilizar un dato personal para un fin concreto, se encuentra habilitado por alguna de las bases de legitimación previstas en el *RGPD*.

3.1.1. Interés público o poderes públicos y cumplimiento de obligación legal

El *RGPD* diseña un sistema de legitimación basado en seis bases jurídicas que no mantienen entre sí ninguna relación de prioridad o prelación. Entre esas bases jurídicas no se encuentran, en sentido estricto, los "fines propios de las Administraciones públicas en el ejercicio de sus competencias" ni la "autorización legal".

En particular, y en el ámbito del INSS, las bases jurídicas que legitiman la mayoría de sus tratamientos son las siguientes:

1. El tratamiento es necesario para el **cumplimiento de una obligación legal** aplicable al responsable del tratamiento.
2. El tratamiento es necesario para el **cumplimiento de una misión realizada en interés público** o en el **ejercicio de poderes públicos conferidos** al responsable del tratamiento.

En ambos casos, debe existir una previsión normativa con rango de ley que habilite a ello, siendo esta, y para el caso concreto de nuestra Entidad:

- El **Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social (TRLGSS),** y respecto los tratamientos de datos personales incardinados en la actividad de gestión de las prestaciones del Sistema de Seguridad Social;
- El **Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido del Estatuto Básico del Empleado Público (TREBEP),** respecto de los tratamientos de datos personales relacionados con las actividades de gestión de los recursos humanos del personal funcionario.
- El **Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (TRLET),** respecto de los tratamientos de datos personales relacionados con las actividades de gestión de los recursos humanos del personal laboral.

EJEMPLOS BASES LEGITIMACIÓN TRATAMIENTOS DEL INSS:

- **Incapacidad Permanente: TRLGSS**
- **Jubilación: TRLGSS**
- **Incapacidad Temporal: TRLGSS**
- **Asistencia Sanitaria: TRLGSS**
- **Formación: TREBEP y TRLET**
- **Acción Social: TREBEP y TRLET**
- **Procesos cobertura de puestos de trabajo: TREBEP y TRLET**
- **Videovigilancia y Seguridad: TREBEP y TRLET**

3.1.2. Consentimiento

En los casos en que la base jurídica de los tratamientos sea el consentimiento, éste deberá tener las características previstas por el *RGPD*, que exige que sea informado, libre, específico y otorgado por los afectados mediante una manifestación que muestre su voluntad de consentir o mediante una clara acción afirmativa.

REQUISITOS DEL CONSENTIMIENTO:

- **Informado: se le facilite la información relacionada con los fines**
- **Libre: no sea impuesto o coaccionado**
- **Específico: se otorgue para el fin concreto perseguido**
- **Otorgado: exista una manifestación expresa del interesado**

Los consentimientos conocidos como "tácitos", basados en la inacción de los afectados, dejaron de ser válidos el 25 de mayo de 2018, incluso para tratamientos iniciados con anterioridad. En estos casos, se ha debido encontrar una base jurídica adecuada dentro de las que ofrece el RGPD.

Como se ha expuesto anteriormente, en el INSS, las bases de legitimación para la mayoría de sus tratamientos vienen constituidas porque el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, o porque el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

No obstante, y siempre con carácter residual, existen algunos tratamientos en los que se ha de pedir el consentimiento de los ciudadanos al no poderse aplicar las bases usuales utilizadas por el INSS, como es el caso de la recogida del número del teléfono móvil o de la dirección del correo electrónico, o el envío de comunicaciones de carácter informativo (publicitario). En estos casos el consentimiento debe ser "inequívoco", lo que supone que se preste mediante una manifestación del interesado o mediante una clara acción afirmativa. Así, no se consideran formas válidas de obtener el consentimiento el uso de casillas ya marcadas o la inacción, en cambio, sí son acordes, la utilización de una declaración por escrito, o la marcación de casillas en un formulario o en un sitio web de Internet.

El Instituto Nacional de la Seguridad Social solicita su consentimiento para utilizar el teléfono móvil, el correo electrónico y datos de contacto facilitados en esta solicitud para enviarle comunicaciones en materia de Seguridad Social.

☐ SÍ doy mi consentimiento

☐ NO doy mi consentimiento

Por lo tanto, el consentimiento en aquellos supuestos en los que este sea la única base de legitimación, se caracterizará por lo siguiente:

- ✓ Puede ser para uno o varios fines. En este caso:

A. *Es posible agruparlos en virtud de su vinculación (por ejemplo, consentimiento para la recepción de publicidad propia o de terceros).*
B. *Pero deberían desagregarse cuando los tratamientos impliquen conductas distintas (por ejemplo tratamiento por quien recaba los datos y cesión a terceros);*

- ✓ Debe ser prestado de forma libre;
- ✓ Revocable;
- ✓ El responsable debe poder probar en todo momento que ha obtenido el consentimiento;
- ✓ Utilizar un lenguaje claro y sencillo.

EJEMPLOS DE TRATAMIENTOS QUE REQUIEREN CONSENTIMIENTO

- La obtención del teléfono móvil para facilitar la cita previa.
- La obtención del correo electrónico para comunicaciones electrónicas.
- Envío de cartas o SMS de campañas informativas publicitarias.

Por otra parte, es muy importante tener en cuenta que si se usa para obtenerlo una declaración escrita, en esta debe quedar claramente diferenciada la parte referente a protección de datos del resto de declaraciones. Asimismo, en el supuesto de datos sensibles (de carácter especial), el consentimiento, además de inequívoco, ha de ser expreso respecto esos datos y finalidad.

3.1.3. El consentimiento del artículo 28 de la Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas.

Según los apartados 2 y 3 del mencionado artículo 28, conforme la nueva redacción dada por la Disposición final undécima de la LO 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales:

"2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.

Las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.

Cuando se trate de informes preceptivos ya elaborados por un órgano administrativo distinto al que tramita el procedimiento, estos deberán ser remitidos en el plazo de diez días a contar desde su solicitud. Cumplido este plazo, se informará al interesado de que puede aportar este informe o esperar a su remisión por el órgano competente.

3. Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.

Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones Públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación".

Ello implica, que cuando el INSS, en el ejercicio de sus competencias o para el cumplimiento de sus obligaciones legales, requiera acceder a la documentación o datos de la persona física que aparezca como interesada ante un trámite administrativo que esté en curso, podrá recabarlos de aquella otra Administración que los custodie.

No cabrá la oposición del ciudadano a dicha recopilación de información, puesto que el consentimiento del interesado no es la base de legitimación en la cual se amparan los tratamientos de datos personales utilizados por el INSS en el desempeño de sus competencias como entidad gestora de las prestaciones del Sistema de Seguridad Social.

3.1.4. La Potestad de Verificación de la Disposición Adicional Octava de la LO3/2018, de Protección de Datos y Garantía de los Derechos Digitales.

Según la citada disposición adicional:

"Cuando se formulen solicitudes por cualquier medio en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos".

Esta potestad de verificación, debe entenderse con mayor amplitud que las facultades otorgadas por el art. 28 de la Ley 39/2015, ya que en este caso no cabrá oposición expresa del ciudadano, al primar el interés público de la administración para comprobar la veracidad de los datos aportados por el interesado sobre el consentimiento del mismo y su posible oposición.

No obstante, en el supuesto que una norma con rango de ley y de aplicación preferente restrinja el acceso a los datos a los que se pretende acceder para verificar su exactitud, será necesario obtener el consentimiento o autorización del ciudadano para poder acceder a los mismos (P.ej. Los datos tributarios conforme el art. 95 de la Ley General Tributaria).

3.1.5. Tratamientos de categorías especiales de datos.

En principio, como punto de partida, queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o la orientación sexual de una persona física.

No obstante, existen una serie de excepciones, entre otras:

- **El consentimiento explícito del interesado para el tratamiento de dichos datos personales.**
- **El cumplimiento de obligaciones o/y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social.**
- **Por razones de un interés público esencial.**
- **Para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social.**

Tal como se deduce de las posibles bases de licitud para los tratamientos de categoría especial, el INSS, en el ejercicio de su competencias, se encuentra habilitado al uso de dichos datos personales al establecerse en una norma con rango de ley esa obligación legal y potestad pública, como es el texto refundido de la Ley General de la Seguridad Social.

EJEMPLOS:

- Procesos de gestión de las incapacidades permanentes
- Procesos de control de las incapacidades temporales
- Procesos de valoración realizados por las Unidades Médicas

3.2. CUMPLIMIENTO DEL PRINCIPIO DE TRANSPARENCIA: EL DERECHO DE INFORMACIÓN EN LA RECOGIDA DE LOS DATOS PERSONALES.

El RGPD regula el derecho de información en sus artículos 13 y 14, distinguiendo entre la información que se debe facilitar al titular de los datos dependiendo si los datos personales se han obtenido del mismo o no.

Este derecho de información, en aras de la transparencia en el tratamiento de los datos personales, se amplía considerablemente, de tal forma que, entre otros, se deberá informar sobre los siguientes extremos:

- **Los datos de contacto del Delegado de Protección de Datos;**
- **La base jurídica o legitimación del tratamiento;**
- **El plazo o criterios de conservación de la información;**
- **La existencia de decisiones automatizadas o elaboración de perfiles;**
- **La previsión de transferencias de datos a terceros países;**
- **El derecho a presentar una reclamación ante las autoridades de control.**

La información se proporcionará de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. Es por ello por lo que en el INSS se ha procedido a revisar todos los formularios de prestaciones y trámites administrativos competencia de esta entidad para adecuarlos tanto en formato papel como electrónico a las nuevas exigencias normativas.

Esta obligación de informar se debe cumplir sin necesidad de requerimiento alguno, y el responsable deberá poder acreditar con posterioridad que ha sido satisfecha.

Además, en el caso de que los datos no se obtengan del propio afectado, habría que informar a este de una serie de extremos referidos a su origen, categoría, uso…No obstante, el RGPD también regula una serie de supuestos que excepcionan la mencionada obligación de informar al interesado de la recopilación y uso de sus datos cuando se hayan obtenido indirectamente:

- **Cuando el afectado ya disponga de la información;**
- **Cuando la comunicación resulte imposible o suponga un esfuerzo desproporcionado;**
- **Cuando la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros; o**
- **Cuando los datos deban seguir teniendo carácter confidencial por un deber legal de secreto.**

Los procedimientos de recogida de información pueden ser muy variados y, por tanto, los modos de informar a los afectados deben adaptarse a las circunstancias de cada uno de los medios empleados para la recopilación o registro de los datos.

Las características de cada uno de los medios varían en cuanto a extensión, disponibilidad de espacio, legibilidad, posibilidad de vincular informaciones, etc.

Para facilitar este cumplimiento, se recomienda adoptar un modelo de información por capas o niveles, que consiste en lo siguiente:

- En un primer nivel, presentar una información básica (identificación del responsable, finalidad del tratamiento, ejercicio de derechos, origen de los datos, realización de perfiles), de forma resumida, en el mismo momento y medio en que se recojan los datos.

- En un segundo nivel, la información adicional, presentando de forma detallada el resto de informaciones.

EPÍGRAFE	INFORMACIÓN BÁSICA (1ª CAPA, RESUMIDA)	INFORMACIÓN ADICIONAL (2ª CAPA, DETALLADA)
RESPONSABLE *DEL TRATAMIENTO*	Identidad del responsable del tratamiento	Datos de contacto del responsable
		Identidad y datos de contacto del representante
		Datos de contacto del delegado de protección de datos
FINALIDAD *DEL TRATAMIENTO*	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica ampliada
LEGITIMACIÓN *DEL TRATAMIENTO*	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo
		Obligación o no de facilitar datos y consecuencias de no hacerlo
DESTINATARIOS *DE CESIONES O TRANMSFERENCIAS*	Previsión o no de cesiones	Destinatarios o categorías de destinatarios
	Previsión de transferencias, o no, a terceros paises	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones especificas aplicables
DERECHOS *DE LAS PERSONAS INTERESADAS*	Referencia al ejercicio de derechos	Como ejercer los derechos de acceso, rectificaciones, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la autoridad de control
PROCEDENCIA *DE LOS DATOS*	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden fuentes de acceso público
		Categorías de datos que se traten

FUENTE: AEPD

EJEMPLOS DE INFORMACIÓN SUMINISTRADA POR EL INSS:

INFORMACIÓN ADICIONAL SOBRE PROTECCIÓN DE DATOS PERSONALES

RESPONSABLE DEL TRATAMIENTO	***¿Quién es el responsable del tratamiento de sus datos personales?*** Instituto Nacional de la Seguridad Social C/ Padre Damián, 4 CP 28036 Madrid, ESPAÑA https://sede.seg-social.gob.es
DELEGADO DE PROTECCIÓN DE DATOS	***¿Cómo puede contactar con el Delegado de Protección de Datos?*** Dirección del Servicio Jurídico de la Seguridad Social C/ Sagasta, 13 - 6ª Planta CP 28004 Madrid, ESPAÑA https://sede.seg-social.gob.es
FINALIDAD DEL TRATAMIENTO	***¿Para qué utilizaremos sus datos?*** Sus datos serán tratados con la finalidad principal de resolver esta solicitud y de gestionar, en su caso, la prestación reconocida. El tratamiento de sus datos de contacto tendrá como finalidad la realización de comunicaciones y remisión de información en materia de Seguridad Social. Los datos personales proporcionados se conservarán mientras sean necesarios para gestionar su prestación o las de sus posibles beneficiarios así como para otros fines de archivo y estadística pública.
LEGITIMACIÓN DEL TRATAMIENTO	***¿Cuál es la legitimación para el tratamiento de sus datos?*** El tratamiento de los datos se realizará sobre la base del ejercicio de poderes públicos autorizado por una norma legal (Arts. 66, 71, 72, 77 y concordantes Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social, en adelante, TRLGSS). Por lo que respecta a las comunicaciones y envío de informaciones en materia de Seguridad Social, el tratamiento vendrá legitimado por su consentimiento. La negativa a otorgarlo supondrá que no podrá recibir este tipo de envíos, si bien, no impedirá que le podamos informar por dichos canales del estado de sus solicitudes. También le informamos de que no está obligado a facilitar su dirección de correo electrónico y número de teléfono móvil y que, en caso de no facilitarlos, no impedirá el trámite de su solicitud.
DESTINATARIOS DE CESIONES O TRANSFERENCIAS	***¿A quién comunicaremos sus datos?*** Los datos personales obtenidos por el Instituto Nacional de la Seguridad Social en el ejercicio de sus funciones tienen carácter reservado y solo se utilizarán para los fines encomendados legalmente, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión o comunicación tenga por objeto alguno de los supuestos previstos expresamente en el artículo 77 del TRLGSS así como en los supuestos indicados en cualquier otra norma de rango legal. Si se trata de una solicitud basada en normativa internacional, sus datos podrán ser cedidos a los organismos extranjeros competentes para el trámite de su solicitud.
DERECHOS DE LAS PERSONAS INTERESADAS	***¿Cuáles son sus derechos cuando nos facilita sus datos personales?*** Respecto de los datos personales proporcionados, puede ejercitar en cualquier momento y en los términos establecidos por la normativa de protección de datos los derechos de acceso, rectificación, supresión, limitación y oposición, o bien retirar el consentimiento prestado a su tratamiento en los casos que hubiese sido requerido, todo ello mediante escrito presentado en un Centro de Atención e Información de la Seguridad Social (CAISS) o, por correo postal o a través de la sede electrónica de la Seguridad Social, ante el Delegado de Protección de Datos cuyos datos se encuentran en el segundo apartado de esta tabla. Le informamos de que en caso de considerar que su requerimiento no ha sido atendido oportunamente, tiene la posibilidad de presentar una reclamación ante la Agencia Española de Protección de Datos.
PROCEDENCIA	***¿Cómo obtenemos sus datos personales?*** Además de los datos facilitados por usted en su solicitud recabamos otros datos personales de otras administraciones y entidades en cumplimiento de la normativa y con el fin de agilizar y facilitar la actuación administrativa. Estos accesos a datos están amparados en normas con rango de ley.

www.seg-social.es **https://sede.seg-social.gob.es**

	INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS PERSONALES
RESPONSABLE	Instituto Nacional de la Seguridad Social (INSS)
FINALIDAD	Gestión de las prestaciones del Sistema de la Seguridad Social competencia del INSS
LEGITIMACIÓN	Ejercicio de poderes públicos
DESTINATARIOS	Sólo se efectuarán cesiones y transferencias previstas legalmente o autorizadas mediante su consentimiento
DERECHOS	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional
PROCEDENCIA	Recabamos datos de otras administraciones y entidades en los términos legalmente previstos
INFORMACIÓN ADICIONAL	Puede consultar información adicional y detallada en la hoja informativa que se acompaña al presente formulario en el apartado "INFORMACIÓN ADICIONAL SOBRE PROTECCIÓN DE DATOS PERSONALES"

IMPORTANTE: Dentro de su ámbito competencial, las direcciones provinciales pueden establecer nuevos tratamientos para mejorar la gestión ordinaria de su actividad prestacional y administrativa. En la recogida de datos personales de los ciudadanos o de los empleados, **deberán dar cumplimiento al derecho de información**

3.3. La transición del registro de ficheros SIGLA al registro de actividades de tratamientos (RAT).

Con el RGPD desaparece la obligación de notificar e inscribir los antiguos ficheros SIGLA, tanto de responsables públicos como privados, en el Registro de Ficheros de la AEPD, o registro de la autoridad autonómica competente. A cambio, surge la obligación de implementar la creación del Registro de Actividades de Tratamiento.

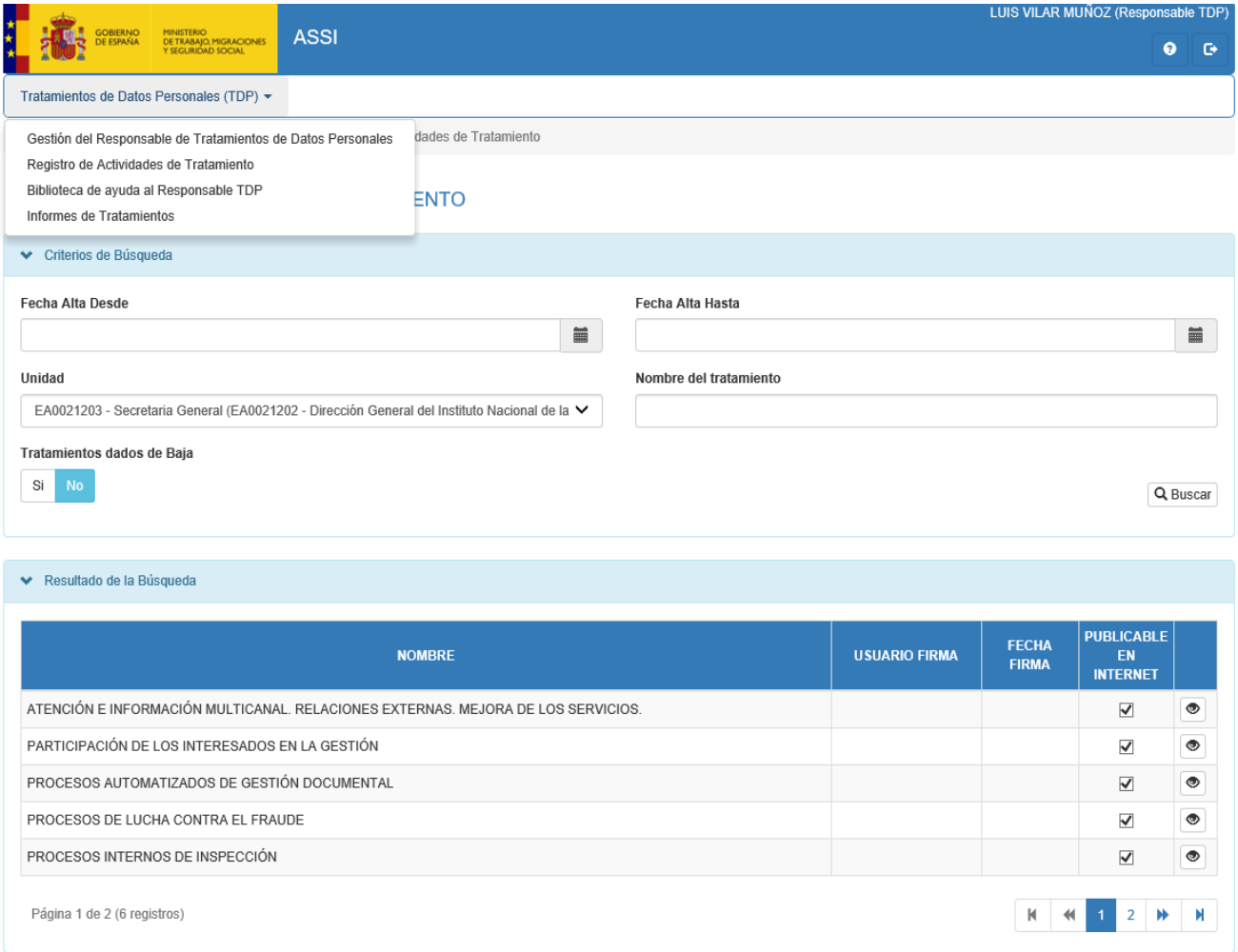
Los responsables y encargados de tratamientos de las Administraciones Públicas deben mantener este Registro de Actividades de Tratamiento por escrito, incluso en formato electrónico, el cual estará a disposición de la Autoridad de Control (AEPD), y en el que se ha de incluir una descripción de los tratamientos de datos que se realicen con la siguiente información:

- **Actividad de Tratamiento.**
- **Nombre y datos de contacto del Responsable**
- **Fines del Tratamiento**
- **Nombre y Datos de contacto del Delegado de Protección de Datos**
- **Categorías de Datos Personales**
- **Categorías de Afectados**
- **Descripción de las Medidas Técnicas y Organizativas de Seguridad**
- **Categorías de destinatarios de comunicaciones, incluidos terceros países u organizaciones internacionales.**

- **Transferencias internacionales: Documentación de Garantías**
- **Plazos previstos para las supresión de las diferentes categorías de datos**

Tras la entrada en vigor de la LOPDGDD el nuevo Registro de Actividades de Tratamientos, no solo ha pasado a ser una obligación impuesta a las AA.PP, sino que además, conforme el artículo 31 de la mencionada ley: *"Los sujetos enumerados en el artículo 77.1 (sector público) de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal".*

En la Administración de la Seguridad Social, se ha utilizado la herramienta informática **ASSI-RGPD** diseñada por el Ministerio de Trabajo, Migraciones y Seguridad Social, para la elaboración del **Registro de Actividades de Tratamientos (RAT),** a fin de lograr una homogeneización en la publicidad de la los tratamientos de actividades realizados por las distintas entidades gestoras y servicios comunes de la Seguridad Social.



El INSS, siguiendo la definición de tratamiento ofrecida por el RGPD y la posibilidad de diseñar el RAT atendiendo a las finalidades perseguidas por los distintos ficheros,

bases de datos y sistemas de información responsabilidad de la Entidad, ha realizado una ardua tarea de análisis y sistematización de los mismos, de tal forma que se ha logrado aglutinar los más de 1300 ficheros existentes en el conjunto de nuestra Entidad, en los 43 tratamientos de actividades publicados en la web y sede electrónica de la Seguridad Social, así como en la intranet de la Seguridad Social:

http://www.seg-social.es (**pestaña Protección de Datos:** Seguridad Social Protección de datos)

Para ello, se decidió centralizar la mencionada labor de análisis y agrupación de todos los ficheros y bases de datos de las 52 de las Direcciones provinciales y los Servicios Centrales, en la Secretaría General, dado su carácter coordinador dentro de la Entidad, y en concreto, en la Inspección de servicios del INSS, por ser la unidad encargada de los programas de protección de datos y de los programas de auditorías de accesos.

REGISTRO ACTIVIDADES TRATAMIENTOS DEL INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL (RAT – INSS)

1. AUXILIO POR DEFUNCIÓN
2. CONTROL DE PENSIONES
3. PLATAFORMA "TU SEGURIDAD SOCIAL"
4. VIUDEDAD NACIONAL
5. PARTICIPACIÓN DE LOS INTERESADOS EN LA GESTIÓN
6. FAVOR DE FAMILIARES INTERNACIONAL
7. TARJETA SOCIAL UNIVERSAL (TSU)
8. PENSIONES EXTRAORDINARIAS DERIVADAS DE ACTOS DE TERRORISMO
9. ORFANDAD NACIONAL
10. ORFANDAD INTERNACIONAL
11. JUBILACIÓN NACIONAL
12. JUBILACIÓN INTERNACIONAL
13. PROCESOS AUTOMATIZADOS DE GESTIÓN DOCUMENTAL
14. PROCESOS DE LUCHA CONTRA EL FRAUDE
15. PROCESOS INTERNOS DE INSPECCIÓN
16. PROCESOS NO AUTOMATIZADOS DE GESTIÓN DOCUMENTAL
17. ATENCIÓN E INFORMACIÓN MULTICANAL. RELACIONES EXTERNAS. MEJORA DE SERVICIOS.
18. GESTIÓN Y PROCESOS DE UNIDADES MÉDICAS
19. EJERCICIO CORRESPONSABLE DEL CUIDADO DEL LACTANTE
20. SÍNDROME TÓXICO
21. SEGURO ESCOLAR
22. RIESGO DURANTE EL EMBARAZO/LACTANCIA NATURAL
23. PROCESOS RELATIVOS AL FONDO ESPECIAL
24. PRESTACIONES FAMILIARES
25. INCAPACIDAD TEMPORAL
26. INGRESO MÍNIMO VITAL
27. CONTROL DE LA INCAPACIDAD TEMPORAL Y OTRAS PRESTACIONES DE CORTA DURACIÓN
28. AYUDA Y CUIDADO DE MENORES A CARGO (CÁNCER Y OT. ENF)
29. NACIMIENTO Y CUIDADO DE MENOR
30. FAVOR DE FAMILIARES NACIONAL
31. GESTIÓN DEL DERECHO A LA ASISTENCIA SANITARIA NACIONAL
32. INCAPACIDAD PERMANENTE NACIONAL
33. INCAPACIDAD PERMANENTE INTERNACIONAL
34. GESTIÓN DEL DERECHO ASISTENCIA SANITARIA INTERNACIONAL
35. VIUDEDAD INTERNACIONAL
36. PROCESOS DE GESTIÓN ECONÓMICA-PRESUPUESTARIA Y ESTUDIOS ECONÓMICOS
37. GESTIÓN DE CONSULTAS, RECURSOS, INDEMNIZACIONES A TANTO ALZADO Y OTROS SUPUESTOS DE RESPONSABILIDAD
38. VIDEOVIGILANCIA Y SEGURIDAD
39. ELIMINACIÓN DE SERIES DOCUMENTALES
40. FORMACIÓN
41. GESTIÓN DE LOS RECURSOS HUMANOS
42. PROCESOS DE REGISTRO Y ARCHIVO
43. SALUD LABORAL Y PREVENCIÓN DE RIESGOS LABORALES

El resultado, como ya se ha dicho, ha sido la confluencia de los 1300 ficheros y bases de datos declaradas, en los 43 tratamientos de datos personales inventariados a través del aplicativo ASSI-RGPD. Así mismo, y para un mejor seguimiento de esa transición entre ficheros SIGLA y tratamientos actividades RAT, se ha elaborado y enviado a cada Dirección provincial su correspondiente tabla de equivalencias para que puedan localizar fácilmente los tratamientos en los que han quedado englobados sus respectivos ficheros.

EJEMPLO TABLA EQUIVALENCIA FICHEROS SIGLA – TRATAMIENTOS RGPD

NOMBRE DEL FICHERO	NOMBRE DEL TRATAMIENTO
Actuaciones del EVI para Entidades Ajenas	GESTIÓN Y PROCESOS DE UNIDADES
Archivo/expedientes	PROCESOS DE REGISTRO Y ARCHIVO
Art. 128 y 131 (CONTROLIT)	CONTROL DE LA INCAPACIDAD TEMPORAL Y OTRAS PRESTACIONES DE CORTA
Bases de cotización minería del carbón	PROCESOS AUTOMATIZADOS DE GESTIÓN DOCUMENTAL
Bases reguladoras de minería del carbón	PROCESOS AUTOMATIZADOS DE GESTIÓN DOCUMENTAL
Control de acceso a expedientes sartido. CAE Sartido	PROCESOS INTERNOS DE INSPECCIÓN
Cambio de Contingencia de IT	CONTROL DE LA INCAPACIDAD TEMPORAL Y OTRAS PRESTACIONES DE CORTA
CIAG. Fondo Especial	PROCESOS RELATIVOS AL FONDO ESPECIAL
CIAG. MÉJICO	PROCESOS DE REGISTRO Y ARCHIVO

3.4. SEGURIDAD EN EL TRATAMIENTO DE LOS DATOS PERSONALES

La protección de los derechos y libertades de los ciudadanos en relación con el tratamiento de sus datos personales que lleve a cabo el INSS, exige la adopción de medidas técnicas y organizativas con la finalidad de garantizar el cumplimiento de lo dispuesto en el RGPD y la LOPDGDD.

Asimismo, la norma europea introduce el análisis de riesgos con la finalidad de evaluar el riesgo que implica el tratamiento de datos personales, y regula las comunicaciones de quiebras de seguridad, tanto respecto a los ciudadanos afectados como a la AEPD.

3.4.1. Análisis de Riesgos

El RGPD obliga a que los responsables lleven a cabo una valoración del riesgo de los tratamientos que realicen, con el fin de establecer las medidas a aplicar. Este análisis del riesgo variará en función de:

- Los tipos de tratamiento.
- La naturaleza de los datos.
- El número de afectados.
- La cantidad y variedad de tratamientos que realice una misma organización.

A través de este análisis de riesgo, se logra determinar las medidas a aplicar para que los tratamientos de datos sean respetuosos con lo dispuesto en el RGPD, además de adoptar las correspondientes medidas de seguridad.

3.4.2. Implementación de medidas de seguridad

El RGPD no establece medidas de seguridad estáticas, por lo que corresponde al responsable determinar aquellas medidas de seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales.

El Título VIII del Real Decreto 1720/2007 (que **sigue vigente**) establece unos controles mínimos de obligado cumplimiento para garantizar la seguridad de los datos, controles que se han de incorporar a las medidas de seguridad a tener en cuenta con el RGPD dentro de los procesos de análisis de riesgos, es decir, las medidas de seguridad ya existentes se deben de mantener y revisar en el marco de dichos procesos.

Así, según el artículo 32 del RGPD las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo se definen en función del estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas.

En definitiva, el primer paso para determinar las medidas de seguridad será la evaluación del riesgo a la que anteriormente nos hemos referido. Una vez evaluado el riesgo, será necesario determinar las medidas de seguridad encaminadas para reducir o eliminar los riesgos para el tratamiento de los datos.

Por otra parte, lo previsto en el Esquema Nacional de Seguridad es aplicable a cualquier información de las Administraciones Públicas sin distinción del soporte en el que se encuentre, por lo que en cuanto a las medidas de seguridad se refiere, este esquema es acorde al enfoque de riesgo del RGPD y se constituye en una herramienta válida para la gestión del riesgo y la adopción de las medidas de seguridad en las citadas Administraciones.

3.4.3. Comunicación de una Brecha de Seguridad de los Datos Personales

Conforme el **Esquema Nacional de Seguridad (ENS)** y la **Directiva NIS**, se puede definir un **"incidente de seguridad"** como aquel evento o serie de eventos, inesperados o no deseados, con consecuencias negativas para la seguridad del sistema de información, y que, con una gran probabilidad, van a comprometer las operaciones de la organización y a amenazar la seguridad de la información, teniendo efectos adversos en la seguridad de las redes y sistemas de información.

No obstante, a efectos de protección de datos, solo resultan de interés aquellos incidentes de seguridad que deban considerarse como una **"brecha de seguridad".**

Un incidente de seguridad constituirá una brecha de seguridad cuando cumpla todas las condiciones siguientes:

1. **Afecte a la seguridad de información,** es decir, ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
2. **Afecte a datos personales.**
3. **Suponga un riesgo** para los derechos y libertades de las personas físicas titulares de los datos.

Las brechas de seguridad pueden producirse tanto en sistemas informáticos (aplicativos informáticos, bases de datos, ficheros informáticos, tabletas, PCs, teléfonos móviles, cds, memorias de almacenamiento, etc.), como en tratamientos en papel (formularios o expedientes en papel, carpetas o archivadores a-z, radiografías, pruebas médicas, titulaciones académicas …).

EJEMPLOS DE BRECHAS DE SEGURIDAD

Acceso por persona no autorizada a expedientes o datos personales:

- Acceso por parte de un funcionario a sistemas de información titularidad del INSS (SARTIDO, Registro de Prestaciones Sociales Públicas, ATRIUM, INCA, etc.) para visualizar los datos personales de un ciudadano cuyo trámite administrativo no nos corresponda.
- Acceso por parte de un funcionario a sistemas de información titularidad de otras Administraciones Públicas (ATT61, Fichero General de Afiliación, Historias clínicas de los Servicios públicos de salud, sistema de información del SEPE, Sistema de Verificación de Identidad y Residencia (SVIR), etc.) para visualizar los datos personales de un ciudadano cuyo trámite administrativo no nos corresponda.
- Acceso por particulares a información con datos personales pertenecientes a terceros (envío postal de documentación a un tercero, entrega de documentación clínica a otro ciudadano, etc.

Pérdida o destrucción de información con datos personales:

- Sustracción de un portátil o tablet corporativa.
- Olvido de un expediente en la cafetería, juzgado o metro.
- Inutilización de un dispositivo por inundación o incendio.
- Perdida de un dispositivo electrónico o de documentación en una mudanza.

Alteración accidental o ilícita de datos personales:

- Cambio de la fecha de nacimiento en una base datos o aplicativo de trámite de prestaciones.
- Rehabilitación de una pensión de persona fallecida constando su muerte.
- Inclusión consciente de miembros de la unidad familiar que no existen.

La normativa vigente impone al responsable del tratamiento (INSS) la **obligación de notificar a la autoridad de control (AEPD) toda brecha de seguridad** que se haya producido en el ámbito de su competencia, en el **plazo máximo de 72h** desde que haya tenido conocimiento de ello.

Así pues, todo trabajador adscrito o dependiente del INSS que se encuentre ante una brecha de seguridad, **deberá comunicarlo a la mayor brevedad posible**, conforme el siguiente procedimiento:

1. Informará a la persona titular de la Subdirección provincial y a la persona responsable en materia de protección de datos de la Dirección provincial, de la situación producida. En el caso de haberse producido en los Servicios Centrales, deberá comunicárselo a la persona titular de la Subdirección general, así como al representante designado por la Subdirección general para participar en el Grupo de Trabajo de Protección de Datos en el INSS.
2. Una vez comunicados lo hechos o situación producida a los responsables señalados en el punto anterior, estos deberán confirmar que el incidente en cuestión se trata de una brecha de seguridad.

3. Tras la confirmación de que la situación producida constituya (o pueda constituir) una brecha de seguridad, en el caso de que la misma afecte a bases de datos, ficheros o sistemas de información de carácter informático, el responsable en materia de protección de datos de la Dirección provincial o de la Subdirección general avisará a la UPI provincial o bien al Centro de Desarrollo del INSS (CDINSS) de los hechos para que adopte las medidas oportunas para poner fin a la brecha de seguridad. y para corregir y paliar los efectos nocivos que se hayan podido producir.
4. En el caso de que la brecha de seguridad afecte a bases de datos, ficheros o sistemas de información no automatizados, o automatizados pero no supervisados por la UPI o el CDINSS, el responsable en materia de protección de datos de la Dirección provincial o de la Subdirección general, en coordinación con la persona responsable funcional de los mismos, adoptará las medidas necesarias para poner fin a la brecha, y para corregir y paliar los efectos nocivos que se hayan podido producir.
5. Todo lo expuesto en los puntos anteriores, se deberá comunicar a la mayor brevedad posible, y siempre antes del transcurso de 48 horas desde que se produjo o se tuvo conocimiento de la incidencia, a la Subdelegada de Protección de Datos del INSS a través del buzón de consultas de protección de datos **(consultas.inss-sscc.proteccion-de-datos@seg-social.es**) o al buzón de la Inspección de Servicios (**inspeccion.inss-sscc.sg@seg-social.es**), en ambos casos del INSS. Dicha comunicación se realizará por parte de la persona titular de la Dirección provincial o del responsable en materia de protección de datos de la misma. En el caso de los SS.CC, la comunicación se realizará por parte del responsable en materia de protección de datos de la Subdirección general correspondiente.
6. La comunicación expuesta en el punto anterior, deberá contener la siguiente información:

1. Naturaleza de la brecha de seguridad:
- Brecha de confidencialidad (acceso no autorizado)
- Brecha de integridad (modificación no autorizada)
- Brecha de disponibilidad (desaparición o pérdida)

2. Categorías de afectados:
- Menores o discapacitados.
- Empleados públicos.
- Ciudadanos.

3. Medio por el que se ha materializado la brecha:
- Dispositivo perdido o robado.
- Documentación perdida, robada.
- Correo perdido o abierto.
- Datos personales mostrados al individuo incorrecto.
- Revelación verbal no autorizada de datos personales.
- Eliminación incorrecta de datos personales formato papel.
- Datos personales residuales en dispositivos obsoletos.

4. Nº aproximado de afectados.
5. Categorías de datos comprometidos:
   - Identificativos, DNI, NUSS, NIE.
   - Credenciales de acceso o identificación.
   - Datos de contacto o residencia.
   - Datos económicos o financieros.
   - Datos de salud.
6. Nº registros de datos personales afectados.
7. Posibles consecuencias de la brecha de seguridad sufrida.
8. Medidas adoptadas o propuestas para remediar la brecha.
9. Si se le ha comunicado la brecha al afectado.
10. Fechas en las que han sucedido todos los hechos.

IMPORTANTE: Es fundamental que las brechas de seguridad se comuniquen al buzón indicado en el **plazo máximo de 48h**. Si no se dispone de toda la información, es posible su ampliación con posterioridad. **Las notificaciones a la AEPD solo se realizarán por parte de la Subdelegada de Protección de Datos**.

3.5. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

El RGPD contiene dos principios para la implementación efectiva de la responsabilidad proactiva, como son los de protección de datos desde el diseño y protección de datos por defecto.

El principio de protección de datos desde el diseño supone que la protección de datos ha de estar presente en las primeras fases de concepción de un proyecto y formar parte de la lista de elementos a considerar antes de iniciar las sucesivas etapas de desarrollo.

Por supuesto, estos requisitos se van a traducir en medidas técnicas y organizativas con el objeto de aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento.

Un ejemplo de dichas medidas, que se establece de forma expresa en el RGPD, es que el propio tratamiento incorpore medidas para la seudonimización de los datos personales o la minimización de datos.

¿QUÉ NECESIDAD TENGO?	¿QUÉ BASE DE LEGITIMACIÓN ME HABILITA?	¿QUÉ DATOS PERSONALES NECESITO?	¿CÓMO VOY A REALIZAR EL TRATAMIENTO?	¿QUÉ RIESGOS CONTRAE EL TRATAMIENTO?	¿QUÉ MEDIDAS DE SEGURIDAD APLICARE?
Fin perseguido con el tratamiento	Obligación legal, potestad pública, consentimiento etc.	Recabar solo los datos estrictamente necesarios en relación al fin	Tanto la obtención de los datos, como su utilización y archivo	Riesgos en la confidencialidad disponibilidad e integridad de los datos personales	Establecer las medidas adecuadas para evitar los riesgos

					previstos
EJEMPLO					
Ordenar citación revisiones médicas	Obligación legal y Consentimiento	Datos identificación, nº teléfono móvil	Envío de sms al móvil del ciudadano a citar	Envío de sms a otra persona, violación de la confidencialidad	Asegurar la exactitud del nº tlfn. indicar en el sms solo los datos de la cita, no exponer datos personales…

Por su parte, la **protección de datos por defecto** estriba en que sólo sean objeto de tratamiento los datos personales que sean estrictamente necesarios para cada uno de los fines de tratamiento. Es decir, independientemente del conjunto de datos recogidos por el responsable con el objeto de implementar los distintos servicios que se proporcionan al sujeto de los datos, el responsable ha de compartimentar el uso del conjunto de datos entre los distintos tratamientos, de tal forma que no todos los tratamientos accedan a todos los datos, sino que actúen solo sobre aquellos que sean necesarios y en los momentos en que sea estrictamente necesario.

En particular, se destaca como uno de los principios de protección de datos por defecto que los datos no sean accesibles a un número indeterminado de personas físicas.

Además, debe tenerse en cuenta lo siguiente respecto a la protección de datos por defecto:

- **Recogida de datos: analizar los tipos de datos que se recaban con un criterio de minimización en función de la actividad administrativa.**
- **Tratamiento de los datos: analizar los procesos asociados a dichos tratamientos para que se acceda a los mínimos datos necesarios.**
- **Conservación: implementar una política de conservación de datos que permita, con un criterio restrictivo, eliminar aquellos datos que no sean estrictamente necesarios.**
- **Accesibilidad: limitar el acceso por parte de terceros a dichos datos.**

IMPORTANTE: recuerda pensar siempre en términos de protección de datos. Busca asegurar la confidencialidad, disponibilidad e integridad de los datos personales. Minimiza los datos recabados/utilizados

3.6. EL DELEGADO DE PROTECCIÓN DE DATOS (DPD) EN LA ADMINISTRACIÓN DE LA SEGURIDAD SOCIAL

El RGPD introduce como obligatoria en el ámbito de las Administraciones Públicas la figura del denominado Delegado de Protección de Datos (DPD), quien será una persona con conocimientos especializados en Derecho y en la práctica en materia de protección de datos personales.

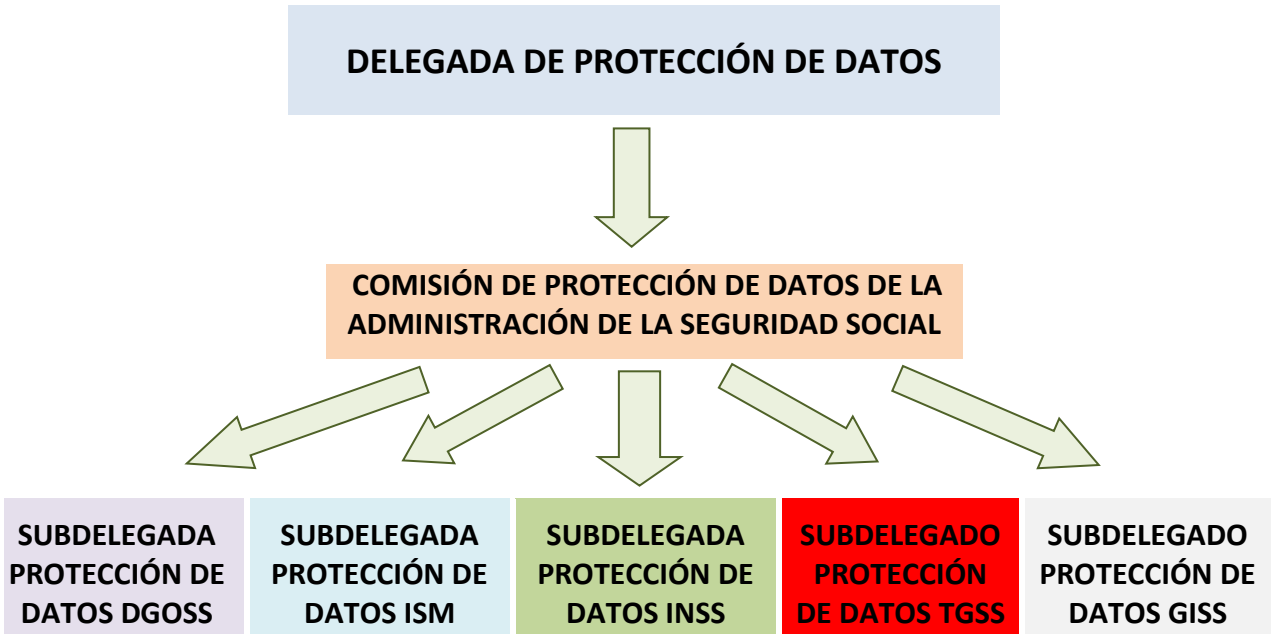
La función del Delegado es **informar, asesorar y supervisar**, siempre bajo la tutela de la Agencia Española de Protección de Datos.

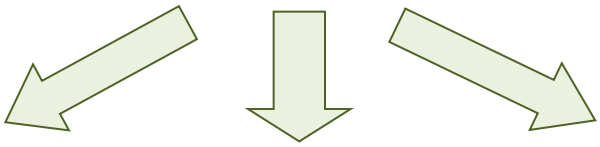
Por otra parte, y dadas las funciones del DPD, su adscripción dentro de la estructura de la organización debe hacerse a órganos o unidades con competencias y funciones de carácter horizontal.

En el ámbito de la Administración de la Seguridad Social, la Resolución de 17 de abril de 2018 de la Secretaría de Estado de la Seguridad Social ha designado como DPD para el conjunto de las Administración de la Seguridad Social, a la persona titular de la Dirección del Servicio Jurídico de la Administración de la Seguridad Social, creando además la Comisión de Protección de Datos de la Administración de la Seguridad Social, integrada por todos los Subdelegados de Protección de Datos que se han designado en cada entidad gestora y servicio común, y cuya principal misión es dar apoyo a la DPD en el ejercicio de sus funciones.

En el caso concreto del INSS, la condición de **Subdelegada de Protección de Datos** ha recaído en la persona titular de la Secretaría General, la cual está asistida dentro de la entidad por:

- El **Grupo de Trabajo de Protección de Datos** del INSS, constituido por representantes de todas las Subdirecciones generales y de la Secretaría general.
- El Área de la **Inspección de Servicios**, con el apoyo directo de:
  - La Jefa de la Inspección.
  - Un Jefe de Agrupación.
- Un **responsable provincial** en materia de protección de datos, junto con el/la directora/a provincial.





GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL INSS	INSPECCIÓN DE SERVICIOS DEL INSS	ÁMBITO DE LAS DIRECCIONES PROVINCIALES DEL INSS
(Representantes de todas las Subdirecciones generales)	(La Jefa de la Inspección y un jefe de Agrupación)	(El/la Responsable en materia de protección de datos)

Como funciones materiales más destacables llevadas a cabo bajo la responsabilidad de la Subdelegada de Protección de Datos del INSS destacan:

- Informar y asesorar a los responsables o encargados del tratamiento y a los empleados que se ocupan del tratamiento, de las obligaciones que les incumben en materia de protección de datos;

- Supervisar el cumplimiento de lo dispuesto en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento y las auditorías correspondientes;

- Actuar como punto de contacto con la Delegada de Protección de Datos y con la Agencia Española de Protección de Datos para cuestiones relativas al tratamiento.

Asimismo, la DPD de la Administración de la Seguridad Social es competente para llevar a efecto aquellas otras actividades de información, coordinación, supervisión, formación o consulta que, en materia de protección de datos, considere procedentes para el debido cumplimiento de la normativa de protección de datos en el ámbito del conjunto de las Entidades Gestoras y Servicios Comunes.

IMPORTANTE: Todas las comunicaciones o consultas que se realicen a la Delegada de Protección de Datos o a la AEPD, deberán realizarse a través de la Subdelegada de Protección de Datos. Recuerda utilizar el buzón específico del INSS en materia de protección de datos para toda comunicación o consulta: **consultas.inss-sscc.proteccion-de-datos@seg-social.es**

3.7. TRANSFERENCIAS INTERNACIONALES DE DATOS.

Cuando los datos personales se envían fuera del ámbito del Espacio Económico Europeo, que comprende todos los Estados miembros de la Unión Europea, más Noruega, Islandia y Liechtenstein, se produce una transferencia internacional de datos.

Aunque podría parecer que las transferencias internacionales son poco habituales en el ámbito la Administración de la Seguridad Social, el uso cada vez más frecuente de tecnologías de la información y la comunicación y la movilidad y translación de derechos en materia laboral y sanitaria de los ciudadanos, supone que aumenten las

posibilidades de que se transfieran estos datos fuera del mencionado Espacio Económico Europeo.

En este sentido, el RGPD contiene una serie de supuestos (artículos 45 y 46), que permiten realizar dichas transferencias internacionales sin necesidad de solicitar una autorización previa por parte de las autoridades de protección de datos.

Dependiendo del tipo de prestación, los responsables del respectivo tratamiento de datos en el ámbito del INSS, deberán tener en cuenta esas posibles implicaciones internacionales y la necesidad de que esas transferencias se lleven a cabo sobre la base de los adecuados instrumentos normativos.

IMPORTANTE: La salida del Reino Unido de la Unión Europea ha supuesto importantes cambios en materia de intercambio de información. Recuerda que en el ámbito internacional, las Consejerías laborales de las Embajadas de España son las intermediarias en materia de prestaciones competencia del INSS.

3.8. Confidencialidad y Secreto profesional. Responsabilidades de los usuarios.

Los responsables (INSS) y encargados (GISS) del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este (empleados públicos y privados), están sujetos al deber de confidencialidad. Dicha obligación general se ve complementada a su vez con los deberes de secreto profesional de conformidad con su normativa aplicable (Letrados, médicos inspectores, interinos, etc.)

Estas obligaciones se mantendrán aun después de finalizar la relación del obligado con el responsable o encargado del tratamiento.

IMPORTANTE: El fin de la relación laboral de los empleados con el INSS (por jubilación, fin de la interinidad, traslado a otro organismo, etc.) no supone el fin de la obligación de guardar el secreto de la informaciones que haya conocido durante el tiempo que hayan trabajado en el mismo**, subsisten el deber de confidencialidad y las responsabilidades por su incumplimiento.**

Todos los usuarios que accedan a datos de carácter personal, asumen una serie de responsabilidades:

- **Comunicar diligentemente cualquier incidente que pueda afectar a la seguridad de los datos de carácter personal que maneje.**
- **Utilizar el puesto de trabajo habitual de forma adecuada para los fines relacionados con sus funciones, evitando otros usos que puedan ocasionar daños en el propio equipo o en los datos que manejen.**
- **Custodiar los elementos de identificación y autenticación que le son proporcionados para el acceso a los sistemas informáticos (contraseñas,**

tarjetas, claves, etc.) de forma que no puedan ser conocidos ni utilizados por personal ajeno.

IMPORTANTE: Las tarjetas identificativas, claves de acceso, contraseñas, etc. son de uso privativo y solo deben ser conocidas y utilizadas por el usuario de las mismas**. No deben facilitarse a otros compañeros**. **Bloquea tu pc** cuando no lo estés utilizando. **Protege la documentación física** que estés manejando.

4. DERECHOS DE LOS AFECTADOS

Los afectados, como titulares de sus datos, pueden ejercitar ante el INSS, los derechos de acceso, rectificación, supresión ("derecho al olvido"), oposición y limitación al tratamiento de los mismos.

El responsable del tratamiento (el INSS) deberá responder en el **plazo máximo de un mes.** Este plazo puede prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes, si bien se deberá informar al ciudadano de la citada prórroga en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Si el ciudadano presentase la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el ciudadano solicite que se facilite de otro modo.

Como hemos visto, el RGPD introduce nuevos derechos. De ellos, el que puede ejercerse más frecuentemente en el ámbito del INSS es el de acceso y limitación del tratamiento: debiendo suspenderse el tratamiento de datos cuando los ciudadanos soliciten la rectificación o supresión al responsable hasta que se resuelva su solicitud.

4.1. Características generales

Se trata de derechos cuyo ejercicio es personalísimo, es decir, que sólo pueden ser ejercidos por el titular de los datos, por su representante legal o por un representante acreditado, de forma que el responsable del tratamiento puede denegar estos derechos cuando la solicitud sea formulada por persona distinta del afectado y no se acredite que actúa en su representación.

Estos derechos se caracterizan por lo siguiente:

- **Su ejercicio es gratuito.**
- **Si las solicitudes son manifiestamente infundadas o excesivas (carácter repetitivo) el responsable podrá cobrar un canon o negarse a actuar.**
- **Deben responderse en el plazo de un mes, pudiéndose prorrogar otros dos meses más, teniendo en cuenta la complejidad y número de las solicitudes.**
- **El responsable está obligado a informar sobre los medios para ejercitar estos derechos. Estos medios deber ser accesibles, no pudiéndose denegar este derecho por el solo motivo de que se opte por otro medio.**

- **Si el responsable no da curso a la solicitud, informará a más tardar en un mes, de las razones y la posibilidad de reclamar ante la AEPD.**
- **Se pueden ejercitar directamente o por medio de representante legal.**
- **Cabe la posibilidad de que por cuenta del responsable, sea el encargado el que atienda la solicitud, si ambos lo han establecido en el contrato o acto jurídico que les vincule.**

Derechos de RGPD	¿En que consisten los derechos de los afectados?
Derecho de acceso	**A que el afectado sea informado de:** • Los fines del tratamiento; categorías de datos personales que se traten y de las posibles comunicaciones de datos y sus destinatarios. • De ser posible, el plazo de conservación de tus datos. De no serlo, los criterios para determinar este plazo. • Del derecho a solicitar la rectificación o supresión de los datos, la limitación al tratamiento, u oponerse al mismo. • Del derecho a presentar una reclamación ante la Autoridad de Control. • Obtener una copia de los datos objeto del tratamiento. • Si se produce una transferencia internacional de datos, recibir información de las garantías adecuadas. • De la existencia de decisiones automatizadas (incluyendo perfiles), la lógica aplicada y consecuencias de este tratamiento. • Debe distinguirse del derecho de acceso de los interesados a los expedientes administrativos que regula la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, así como del derecho de acceso regulado en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
Derecho de rectificación	• Rectificar los datos inexactos, y a que se completen los datos personales incompletos, inclusive mediante una declaración adicional.
Derecho de supresión ("Derecho al olvido")	**Con su ejercicio el afectado puede solicitar:** • La supresión de los datos personales sin dilación debida cuando concurra alguno de los supuestos contemplados. Por ejemplo, tratamiento ilícito de datos, o cuando haya desaparecido la finalidad que motivó el tratamiento o recogida. • No obstante, se regulan una serie de excepciones en las que no procederá este derecho. Por ejemplo, cuando deba prevalecer el derecho a la libertad de expresión e información.
Derecho a la limitación del tratamiento	**Permite al afectado:** 1. Solicitar al responsable que suspenda el tratamiento de datos cuando: • Se impugne la exactitud de los datos, mientras se verifica dicha exactitud por el responsable; • El afectado ha ejercitado su derecho de oposición al tratamiento de datos, mientras se verifica si los motivos legítimos del responsable prevalecen sobre el afectado. 2. Solicitar al responsable que conserve tus datos personales cuando: • El tratamiento de datos sea ilícito y el afectado se oponga a la supresión de sus datos y solicite en su lugar la limitación de su uso; • El responsable ya no necesita los datos para los fines del tratamiento pero el afectado si los necesite para la formulación, ejercicio o defensa de reclamaciones.
Derecho de oposición	**El afectado puede oponerse al tratamiento:** • Cuando por motivos relacionados con su situación personal, debe cesar el tratamiento de tus datos salvo que se acredite un interés legítimo, o sea necesario para el ejercicio o defensa de reclamaciones. • Cuando el tratamiento tenga por objeto la mercadotecnia directa.

Fuente: AEPD

4.2. DERECHO DE ACCESO (Artículos 15 RGPD y 13 LOPDGDD)

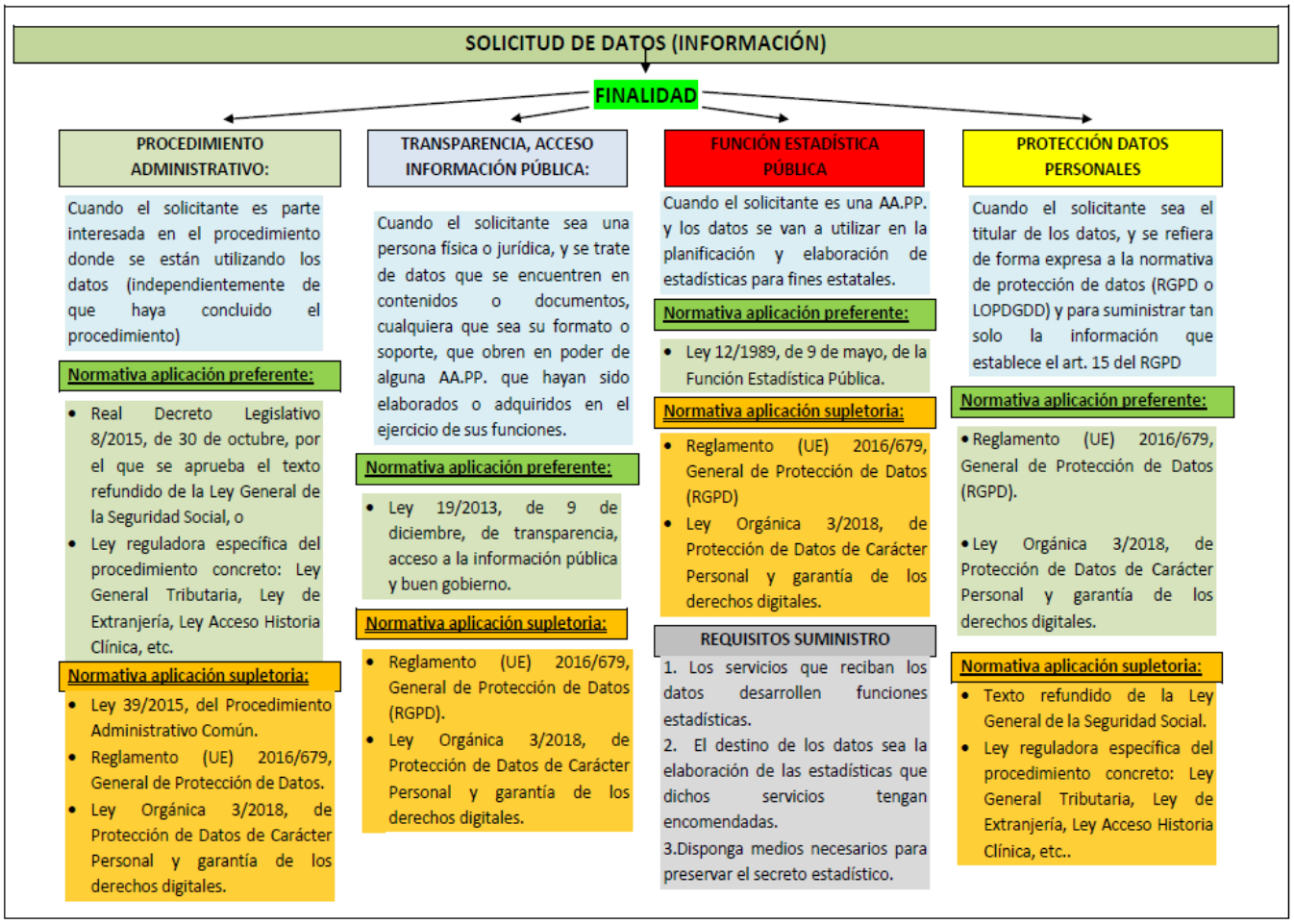
Supone el derecho a dirigirse al responsable del tratamiento para conocer si se están tratando o no datos de carácter personal y, en caso de que se esté realizando dicho tratamiento, obtener información sobre:

- Los fines del tratamiento
- Obtener copia de los datos personales que son objeto de tratamiento
- Las categorías de datos personales de que se trate
- Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros países u organizaciones internacionales
- De ser posible, el plazo previsto de conservación de los datos personales o, si no es posible, los criterios utilizados para determinar este plazo
- Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.
- El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. La comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.
- Se podrá considerar repetitivo el derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.

IMPORTANTE: No debe confundirse el **derecho de acceso** en materia de **protección de datos** con el derecho de acceso al **expediente administrativo**, el derecho de acceso a la **información pública** o el derecho de acceso a la **historia clínica; son derechos de acceso diferentes,** con legitimaciones e interesados distintos.

En las solicitudes de acceso a información debe prestarse una especial atención al motivo o finalidad invocada por el peticionario de la solicitud para poder distinguir cual es la base legal que habilita dicha cesión de información.

Ver esquema siguiente:



4.3. DERECHO DE RECTIFICACIÓN (Artículos 16 de RGPD y 14 de LOPDGDD)

Al ejercer el derecho de rectificación el interesado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse.

Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto del tratamiento.

4.4. DERECHO DE SUPRESIÓN (Artículos 17 del RGPD y 17 de LOPDGDD)

Se podrá ejercitar este derecho ante el responsable solicitando la supresión de los datos de carácter personal cuando concurra alguna de las siguientes circunstancias:

Si los datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo

Si el tratamiento de los datos personales se ha basado en el consentimiento que se prestó al responsable y, se retira el mismo, siempre que el citado tratamiento no se base en otra causa que lo legitime

Este derecho no es ilimitado, de tal forma que puede no llevarse a cabo la supresión cuando el tratamiento sea necesario para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, por razones de interés público, en el ámbito de la salud pública, con fines de archivo de interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

IMPORTANTE: En el **ámbito del INSS** este derecho solo tendrá lugar ante tratamientos que se hayan basado en el consentimiento del ciudadano (p.ej. obtener el teléfono móvil o el correo electrónico). En el resto de tratamientos, **no se pueden suprimir los datos**, tan solo procederá su bloqueo para limitar el acceso a los mismos.

4.5. DERECHO DE OPOSICIÓN (Artículos 21 del RGPD y 18 de la LOPDGPD)

Este derecho supone que el interesado se puede oponer a que el responsable realice un tratamiento de los datos personales en los siguientes supuestos:

Cuando sean objeto de tratamiento basado en una misión de interés público o en el interés legítimo, incluido la elaboración de perfiles. El responsable dejará de tratar los datos salvo que acredite motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Cuando el tratamiento tenga como finalidad la mercadotecnia directa, incluida también la elaboración de perfiles. Ejercitado este derecho para esta finalidad, los datos personales, dejarán de ser tratados para dichos fines

4.6. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO (Artículos 18 del RGPD y 16 de la LOPDGPD)

Este nuevo derecho consiste en obtener la limitación del tratamiento de los datos que realiza el responsable, si bien su ejercicio presenta dos vertientes:

Se puede solicitar la suspensión del tratamiento de los datos:

- Cuando se impugne la exactitud de los datos personales, durante el plazo que permita al responsable su verificación;
- Cuando el interesado se haya opuesto al tratamiento de los datos personales que el responsable realiza en base al interés legítimo o misión de interés público, mientras aquel verifica si estos motivos prevalecen sobre los del interesado.

Solicitar al responsable la conservación de los datos:

- Cuando el tratamiento sea ilícito y el interesado se ha opuesto a la supresión de sus datos y en su lugar solicita la limitación de su uso;
- Cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

4.7. DERECHO A LA PORTABILIDAD DE LOS DATOS (Artículos 20 del RGPD y 17 de la LOPDGPD)

La finalidad de este nuevo derecho es reforzar aún más el control de los datos personales, de forma que cuando el tratamiento se efectúe por medios automatizados, el interesado pueda recibir los datos personales en un formato estructurado, de uso común, de lectura mecánica e interoperable y pueda transmitirlos a otro responsable del tratamiento, siempre que el tratamiento se legitime en base al consentimiento o en el marco de la ejecución de un contrato.

Este derecho no ese puede aplicar cuando el tratamiento sea necesario para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable.

IMPORTANTE: Este derecho **no es aplicable a los tratamientos realizados por el INSS** con independencia de las bases de legitimación de los mismos. No debe confundirse con el derecho de acceso al expediente administrativo o a la historia clínica.

4.8. DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS (Artículos 22 del RGPD y 18 de la LOPDGPD)

Este derecho pretende garantizar que una persona no sea objeto de una decisión basada únicamente en el tratamiento de sus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre ella o le afecte significativamente de forma similar.

La elaboración de perfiles consiste en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales, en particular aquellos que analicen o predigan aspectos relacionados con el rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o el comportamiento.

Este derecho no será aplicable cuando:

- Sea necesario para la celebración o ejecución de un contrato entre una persona y el responsable.
- El tratamiento de los datos se fundamente en el consentimiento prestado previamente.

En estos dos supuestos, el responsable debe garantizar el derecho a obtener la intervención humana, a expresar el punto de vista e impugnar la decisión.

IMPORTANTE: Este derecho **no es aplicable a los tratamientos realizados por el INSS**, ya que siempre se garantiza la intervención humana en las decisiones que se adoptan por la entidad. Toda resolución, reclamación o demanda realizada por la entidad se lleva a cabo bajo la supervisión de una persona física.

4.9. PROCEDIMIENTO DE ACTUACIÓN ANTE SOLICITUDES DE EJERCICIO DE DERECHOS

Instrucciones comunes

1. Cuando un ciudadano desee ejercitar alguno de los derechos, **se le facilitará el modelo correspondiente** *(ver anexo I: Modelos de solicitud derechos)*. Una vez cumplimentado se registrará y se enviará al responsable provincial en materia de protección de datos para su tramitación, quien recabará el apoyo de la unidad competente. La unidad competente se determinará por la ubicación del fichero, base de datos o sistema de información, y trámite afectado.

   Además del modelo oficial, los usuarios **podrán presentar su propia solicitud** siempre que cumpla, como mínimo, **los siguientes requisitos:**

   - Nombre y apellidos del interesado
   - Fotocopia del DNI, pasaporte, o NIE. También la de la persona que lo representa cuando se actúe en representación. Si la solicitud se realiza por medios telemáticos, se acreditará a través de la firma electrónica
   - Dirección a efectos de notificaciones
   - Petición en que se concreta la solicitud
   - Fecha y firma

2. Una vez presentada, **se entregará al interesado una copia sellada** de la solicitud.
3. **Si la solicitud no reúne los requisitos** especificados en el apartado 1, se deberá solicitar la subsanación de los mismos. El **plazo fijado para la subsanación será de 10 días**. De no presentarla en el citado plazo, se considerará como desistida su petición, conforme establecen los artículos 68 y 69 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
4. Si la solicitud se refiere a ficheros o bases de datos personales que no son responsabilidad del INSS, **deberá remitirse a la institución u organismo competente**, comunicando al interesado dicha circunstancia y la fecha del traslado.

5. La Dirección provincial donde se haya presentado la solicitud para el ejercicio de los derechos, **resolverá en el plazo de un mes.**
6. En **caso de dudas sobre como tramitar la solicitud**, se recabará el asesoramiento de la Subdelegada de Protección de Datos a través del **buzón de consultas corporativo**: **consultas.inss-sscc.proteccion-de-datos@seg-social.es**
7. Si la petición se desestima, se informará al interesado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos (AEPD).

4.10. TUTELA DE LOS DERECHOS ANTE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS *(Sede electrónica de la AEPD)*

En el caso de que el responsable del fichero no haya atendido su solicitud en los plazos marcados por la Ley, tanto el RGPD como la LOPDGDD contemplan la posibilidad de que el ciudadano pueda reclamar la asistencia de la Agencia Española de Protección de Datos (AEPD) para que el ejercicio de sus derechos sea efectivo, mediante la presentación de una Reclamación de Tutela de Derechos.

El Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD), pone a disposición varios mecanismos para la resolución de las cuestiones relativas al tratamiento de los datos personales y al ejercicio de los derechos.

Si una persona alberga dudas acerca de dicho tratamiento puede dirigirse directamente al responsable del tratamiento (INSS), a través de los canales de contacto previstos por este, donde puede asimismo ejercitar sus derechos, los cuales deben ser atendidos de forma gratuita, según lo previsto en el artículo 12 del RGPD.

En el caso de que el responsable no haya resuelto las cuestiones planteadas, se puede alcanzar una solución amistosa, contemplada en el artículo 38 del RGPD, poniéndose en contacto con el Delegado de Protección de Datos (DPD) que, en su caso, haya designado el responsable o el encargado de tratamiento, entre cuyas funciones figura la de supervisar el cumplimiento de la normativa de protección de datos.

También se puede hacer uso de los mecanismos de mediación, procedimientos extrajudiciales y otros procedimientos de resolución de conflictos, previstos en el artículo 40 del RGPD, para resolver las controversias surgidas con los responsables del tratamiento.

Finalmente y sin perjuicio de las acciones ejercitables ante los Tribunales de Justicia, contempladas en el artículo 79 del RGPD, se puede presentar una reclamación ante una Autoridad de control, de acuerdo con lo señalado en el artículo 77.

Si la reclamación se refiere a un asunto competencia de alguna de las Autoridades autonómicas de Protección de Datos (País Vasco, Cataluña o Andalucía), la AEPD da traslado de la misma e informa al interesado.

El plazo máximo de resolución de la reclamación es de tres meses.

5. PREGUNTAS FRECUENTES

5.1. TRATAMIENTO DE DATOS EN EL MARCO FUNCIONARIAL Y LABORAL

- **¿Se pueden comunicar a los representantes de los trabajadores datos de carácter personal del personal que presta sus servicios en el INSS?**

Como se ha expuesto anteriormente, uno de los supuestos que habilitan el tratamiento de datos personales es en el cumplimiento de una obligación legal impuesta al responsable del tratamiento (INSS).

Si se tratan de **datos referidos a personal funcionario**, la comunicación vendría habilitada de la siguiente forma:

El Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público, en su artículo 39.1 establece que “Los órganos específicos de representación de los funcionarios son los Delegados de Personal y las Juntas de Personal”, según proceda.

Por otro lado, en el artículo 40 enumera las funciones atribuidas a las Juntas de Personal y a los Delegados de Personal:

a. Recibir información, sobre la política de personal, así como sobre los datos referentes a la evolución de las retribuciones, evolución probable del empleo en el ámbito correspondiente y programas de mejora del rendimiento.
b. Emitir informe, a solicitud de la Administración Pública correspondiente, sobre el traslado total o parcial de las instalaciones e implantación o revisión de sus sistemas de organización y métodos de trabajo.
c. Ser informados de todas las sanciones impuestas por faltas muy graves.
d. Tener conocimiento y ser oídos en el establecimiento de la jornada laboral y horario de trabajo, así como en el régimen de vacaciones y permisos.
e. Vigilar el cumplimiento de las normas vigentes en materia de condiciones de trabajo, prevención de riesgos laborales, Seguridad Social y empleo y ejercer, en su caso, las acciones legales oportunas ante los organismos competentes.
f. Colaborar con la Administración correspondiente para conseguir el establecimiento de cuantas medidas procuren el mantenimiento e incremento de la productividad.

A la vista de la previsión legal que se acaba de citar, las funciones atribuidas a las Juntas de Personal por el Real Decreto Legislativo 5/2015, de 30 de octubre, pueden llevarse con un adecuado desarrollo sin necesidad de proceder a una cesión masiva de los datos referentes al personal que presta sus servicios en el Órgano o Dependencia correspondiente, salvo que hubieran dado su consentimiento, y ello derivado de que, con carácter general, la cesión de datos no está contemplada específicamente en el Estatuto Básico del Empleado Público.

No obstante lo anterior, en el supuesto en que un empleado público haya planteado una queja ante su sección sindical, comité o junta correspondiente, relativa a sus condiciones de trabajo, será posible la cesión del dato específico de dicha persona.

Si se trata de **datos referidos al personal laboral**, la comunicación vendría habilitada de la siguiente forma:

El artículo 64 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, en materia de información y consulta de los trabajadores y en materia de protección de los trabajadores asalariados en caso de insolvencia del empresario, recoge las competencias del Comité de Empresa y dispone en su número 1 que: "El comité de empresa tendrá derecho a ser informado y consultado por el empresario sobre aquellas cuestiones que puedan afectar a los trabajadores, así como sobre la situación de la empresa y la evolución del empleo en la misma, en los términos previstos en este artículo.

Se entiende por información la transmisión de datos por el empresario al comité de empresa, a fin de que éste tenga conocimiento de una cuestión determinada y pueda proceder a su examen. (….)"

Y su número 7 apartado a) atribuye a dicho órgano: "Ejercer una labor:

1º De vigilancia en el cumplimiento de las normas vigentes en materia laboral, de Seguridad Social y empleo, así como el resto de los pactos, condiciones y usos de empresa en vigor, formulando, en su caso, las acciones legales oportunas ante el empresario y los organismos o tribunales competentes;

2º De vigilancia y control de las condiciones de seguridad y salud en el desarrollo del trabajo en la empresa, con las particularidades previstas en este orden por el artículo 19 de esta Ley.

3º De vigilancia del respeto y aplicación del principio de igualdad de trato y de oportunidades entre mujeres y hombres.

b) Participar, como se determine por convenio colectivo, en la gestión de las obras sociales establecidas en la empresa en beneficio de los trabajadores o de sus familiares. (…)

Y según el apartado 9 del citado precepto:

Respetando lo establecido legal o reglamentariamente, en los convenios colectivos se podrán establecer disposiciones específicas relativas al contenido y a las modalidades del ejercicio de los derechos de información y consulta previstos en este artículo, así como al nivel de representación más adecuado para ejercerlos."

Por otra parte, también debe tenerse presente que según el artículo 8.4 del Estatuto de los Trabajadores:

4º El empresario entregará a la representación legal de los trabajadores una copia básica de todos los contratos que deban celebrarse por escrito, a excepción de los contratos de relación laboral especial de alta dirección sobre los que se establece el deber de notificación a la representación legal de los trabajadores.

Con el fin de comprobar la adecuación del contenido del contrato a la legalidad vigente, esta copia básica contendrá todos los datos del contrato a excepción del número del documento nacional de identidad o del número de identidad de extranjero, el domicilio, el estado civil, y cualquier otro que, de acuerdo con la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pudiera afectar a la intimidad personal. El tratamiento de la información facilitada estará sometido a los principios y garantías previstos en la normativa aplicable en materia de protección de datos.

La copia básica se entregará por el empresario (INSS), en plazo no superior a diez días desde la formalización del contrato, a los representantes legales de los trabajadores, quienes la firmarán a efectos de acreditar que se ha producido la entrega.

De la norma expuesta podemos concluir, al igual que en el apartado anterior, que existe habilitación legal suficiente para comunicar a la representación legal de los trabajadores los datos necesarios para que puedan ejercer sus funciones, sin necesidad de proceder a una información masiva. Sólo en el supuesto en que la vigilancia o control se refieran a un sujeto concreto, que haya planteado la correspondiente queja ante el Comité de Empresa, será posible la cesión de datos específicos de dicha persona.

En los demás supuestos, la función de control quedará plenamente satisfecha, mediante la comunicación de la información debidamente disociada, de forma que permita al Comité conocer las circunstancias cuya vigilancia le ha sido encomendada sin referenciar la información en un sujeto concreto.

5.2. VIDEOVIGILANCIA

- **¿Cómo se realiza el cumplimiento de la normativa de videovigilancia en la instalación de cámaras de seguridad en los edificios del INSS?**

La imagen es un dato de carácter personal que permite la identificación de personas físicas. La videovigilancia con fines de preservar la seguridad de bienes y personas, supone un tratamiento de datos, y por tanto, está sometida al RGPD.

En líneas generales, los elementos más destacados a efectos de cumplimiento son los siguientes:

- Elaborar el registro de actividades del tratamiento que se realice a través de videovigilancia.
- Cumplir con el derecho de información mediante un cartel en el que se indique, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos de acceso y supresión que regula el RGPD (*ver anexo II*).
- Adoptar las correspondientes medidas de seguridad.

- **¿Se pueden instalar cámaras de videovigilancia que graben la vía pública?**

La instalación de videocámaras en lugares públicos, tanto fijas como móviles, es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad, rigiéndose el tratamiento de dicha imágenes por su legislación específica, contenida en la Ley Orgánica 4/1997, de 4 de agosto, y su Reglamento de desarrollo, sin perjuicio de que les sea aplicable, en su caso, lo previsto por el RGPD, en aspectos como la adopción de las medidas de seguridad que resulten de aplicación y la elaboración del registro de actividades en relación con el tratamiento de videovigilancia que se realice.

Su utilización en lugares públicos tienen una finalidad específica de seguridad en beneficio de la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.

La instalación de este tipo de dispositivos de las imágenes grabadas, está sujeta a requisitos muy estrictos ya que, en primer lugar, la autorización de instalación de videocámaras fijas y la utilización de cámaras móviles se otorga por la Delegación del Gobierno previo informe preceptivo y vinculante de la Comisión de Garantías de la Videovigilancia de la Comunidad Autónoma correspondiente.

5.3. ACCESO A EXPEDIENTES ADMINISTRATIVOS Y LEY DE TRANSPARENCIA

- **Cuando una unidad administrativa del INSS recibe una denuncia de un ciudadano ¿es posible comunicar sus datos al denunciado?**

En el supuesto de que el denunciante haya manifestado expresamente su deseo de confidencialidad o a juicio del departamento que tramita ese expediente se considere necesario garantizar la identidad del denunciante en condiciones de confidencialidad, podrá denegarse al denunciado el acceso a los datos personales del citado denunciante.

En todo caso, esta comunicación al denunciante debería producirse previa ponderación de si la misma resulta necesaria a los efectos de que las personas denunciadas en el expediente puedan ejercer en plenitud sus derechos, conforme a lo requerido por el artículo 5 del RGPD, no debiendo tener dicha comunicación un carácter genérico ni extenderse a la totalidad de los datos que figuren en la denuncia presentada voluntariamente o en el correspondiente boletín de denuncia.

- **¿Se puede facilitar a un tercero el DNI o número de teléfono existente en un expediente administrativo?**

Respecto al acceso a los expedientes administrativos, debemos distinguir lo siguiente:

a) Si el procedimiento administrativo no ha finalizado, en virtud de lo establecido en la Ley 39/2015, sólo podrán acceder a los datos contenidos en los expedientes quienes ostenten la condición de interesado.

b) Si el procedimiento administrativo ha finalizado, el acceso a los datos obrantes en los expedientes se tramitaría conforme a la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno, cuya regla general es conceder

el acceso a la información obrante en la Administración a la cual se ha dirigido la petición.

Ahora bien, dicho derecho no es ilimitado, estableciendo la propia Ley diversos límites en sus artículos 14 y 15, de los que interesa analizar aquí los establecidos en el artículo 15, relativos a la protección de datos de carácter personal.

En cuanto a los datos de DNI o número de teléfono, cabe efectuar la ponderación exigida por el artículo 15, pero también puede acudirse a lo previsto en el número 4 del artículo. De este modo, si se eliminan tales datos de las copias de los documentos que se faciliten, de modo que no pueda saberse quien es la persona cuyos datos personales han sido tratados, no resultaría de aplicación la normativa de protección de datos.

- **¿Y podrían facilitarse datos tributarios obrantes en los expedientes administrativos?**

La Ley 19/2013, dispone que *"Se regirán por su normativa específica, y por esta Ley con carácter supletorio, aquellas materias que tengan previsto un régimen jurídico específico de acceso a la información."*

Este sería el caso de los datos tributarios obrantes en el INSS, en aplicación del artículo 95 de la Ley 57/2003, de 17 de diciembre, General Tributaria, que declara que tales datos tienen carácter reservado y permite ceder los mismos solamente en los casos que taxativamente enumera, por lo que fuera de tales supuestos no cabe su comunicación.

- **¿Se puede notificar la resolución de un procedimiento administrativo de forma conjunta a todos los interesados incluyendo todos sus datos de contacto?**

En este caso no resulta adecuado que los datos de contacto (domicilio, dirección de correo electrónico, número de teléfono) de los interesados sean comunicados al resto aunque figuren en documentos que les deban ser trasladados, ya que podría ser contrario al principio de minimización de datos del RGPD.

- **¿Qué información se puede publicar en relación a la Transparencia?**

La Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, regula en su Capítulo II la denominada "Publicidad activa", estableciendo una serie de supuestos de publicación obligatoria a través de los denominados Portales de Transparencia.

En la medida que pudiese afectar la publicación a datos de carácter personal, la legitimación para dicha publicación vendría dada por el artículo 6.1.c) del RGPD, es decir, el cumplimiento de una obligación legal.

No obstante, debe tenerse en cuenta lo siguiente:

- Serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15 de la Ley

19/2013, de 9 de diciembre. A este respecto, cuando la información contuviera categorías especiales de datos, la publicidad sólo se llevará a cabo previa disociación de los mismos.

- Los afectados por la publicación podría ejercitar el derecho de oposición a la publicación de sus datos, y suponer la supresión de los mismos. Por ejemplo, una persona víctima de violencia de género, que si bien de acuerdo a lo indicado anteriormente se podría realizar la publicación de sus datos meramente identificativos, alega dicha condición en aras de garantizar su seguridad para que esta publicación no se realice.

- **¿Se pueden publicar los datos de los licitadores y actas de las mesas de contratación? ¿Y los miembros de las mesas de contratación y comités de expertos?**

El artículo 63 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, determina una serie de supuestos de publicación obligatoria, que en la medida que afecte a datos de carácter personal, la legitimación se fundamentaría en el artículo 6.1.c) del RGPD relativo al cumplimiento de una obligación legal.

Asimismo, debe considerarse lo siguiente:

- Para la publicación del número e identidad de los licitadores participantes, respecto a personas físicas, además de su nombre y apellidos, será suficiente con publicar las últimas cuatro cifras del NIF.

- Respecto al a publicación de las actas de la mesa de contratación relativas al procedimiento de contratación, no será necesario que en el contenido de las actas objeto de publicación figure las firmas del Presidente y Secretario de la mesa.

- Respecto a la publicación de los miembros de las mesas de contratación y comités de expertos, será suficiente con publicar nombres y apellidos, y cargos de los mismos.

- Al igual que en la pregunta-respuesta anterior, sería posible el ejercicio del derecho de oposición por los afectados.

- **¿Puede el INSS facilitar a un Ayuntamiento o Comunidad Autónoma los datos de las personas que reciben una pensión no contributiva o con complementos a mínimos para que ese Ayuntamiento o Comunidad Autónoma pueda ofrecer a esas personas sus servicios públicos de carácter social?**

Ambas Administraciones, tanto la de carácter autonómico como la de carácter local, ostentan competencias en materia de servicios sociales, es decir, llevan a cabo, a efectos de la legitimación para el tratamiento de datos contemplada en el RGPD, una

misión de interés público o poder público, por lo que aparentemente se le podrían comunicar esos datos personales.

No obstante, los datos obtenidos y custodiados por el INSS tienen el carácter de reservados conforme el **art. 77.1 del TRLGSS**, que establece que solo podrán ser cedidos para:

- La investigación o persecución de delitos públicos por los órganos jurisdiccionales, el Ministerio Público o la Administración de la Seguridad Social.
- La colaboración con las Administraciones tributarias a efectos del cumplimiento de obligaciones fiscales en el ámbito de sus competencias.
- La colaboración con la Inspección de Trabajo y Seguridad Social, en el ejercicio de sus funciones de inspección y control interno o con las demás entidades gestoras de la Seguridad Social distintas del cedente y demás órganos de la Administración de la Seguridad Social y para los fines de estadística pública en los términos de la ley reguladora de dicha función pública.
- La colaboración con cualesquiera otras Administraciones públicas para la lucha contra el fraude en la obtención o percepción de ayudas o subvenciones a cargo de fondos públicos, incluidos los de la Unión Europea, así como en la obtención o percepción de prestaciones incompatibles en los distintos regímenes del sistema de la Seguridad Social .
- La colaboración con las comisiones parlamentarias de investigación en el marco legalmente establecido.
- La protección de los derechos e intereses de los menores o incapacitados por los órganos jurisdiccionales o el Ministerio Público.
- La colaboración con el Tribunal de Cuentas en el ejercicio de sus funciones de fiscalización de la Administración de la Seguridad Social.
- La colaboración con los jueces y tribunales en el curso del proceso y para la ejecución de resoluciones judiciales firmes. La solicitud judicial de información exigirá resolución expresa, en la que, por haberse agotado los demás medios o fuentes de conocimiento sobre la existencia de bienes y derechos del deudor, se motive la necesidad de recabar datos de la Administración de la Seguridad Social.
- La inspección médica de los servicios públicos de salud podrá solicitar la remisión de datos médicos, necesarios para el ejercicio de sus competencias, que obren en poder de las entidades gestoras de la Seguridad Social.

- **¿Puede una Mutua colaboradora de la Seguridad Social solicitar la documentación contenida en un expediente de incapacidad, sin consentimiento del trabajador, para la determinación de la contingencia?**

El INSS deberá facilitar a las mutuas, si así lo solicitan, la documentación e informes contenidos en el expediente de determinación de la contingencia causante de los procesos por incapacidad temporal, incluidos los informes y pruebas médicas realizadas al trabajador, así como el informe preceptivo del EVI/CEI, sin necesidad de solicitar el consentimiento expreso del trabajador.

- **¿Puede e INSS usar el número de teléfono móvil de los ciudadanos para enviar comunicaciones a través de sistemas de mensajería instantánea?**

Uno de los principios relativos al tratamiento que recoge el RGPD es el referente a que los datos personales serán recogidos con fines determinados, explícitos y legítimos, no siendo tratados ulteriormente de manera incompatible con dichos fines.

De esta forma, si el INSS hubiese recabado el dato del teléfono móvil para una finalidad determinada (por ejemplo, para obtener cita previa), el uso de este dato para enviar dichas comunicaciones sería incompatible, por lo que para realizar el citado envío sería necesario el consentimiento previo de los ciudadanos, además de informarles del tratamiento que se va a realizar respecto a ese dato de carácter personal.

- **¿Se debe dar cumplimiento al derecho de información cuando se recaban datos personales a través de llamadas y correos electrónicos?**

El RGPD regula el derecho de información en sus artículos 13 y 14, además de que uno de los principios relativos al tratamiento que recoge la norma es el relativo a la transparencia.

Por tanto, en ambos supuestos se debe dar cumplimiento al derecho de información. Así pues, en el caso telefónico se puede facilitar la información básica mediante una locución clara y concisa, y el resto del contenido de este derecho a través de otro medio adicional que se ponga a disposición del afectado.

En el supuesto del correo electrónico, en la primera comunicación respecto al ciudadano que haya remitido el mismo, se le podría facilitar la información básica y un enlace en el cuál pueda obtener el contenido de la información de la segunda capa.

ANEXO I

FORMULARIO PARA EL EJERCICIO DE DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

MINISTERIO
DE INCLUSIÓN, SEGURIDAD SOCIAL
Y MIGRACIONES

SECRETARÍA DE ESTADO
DE LA SEGURIDAD SOCIAL
Y PENSIONES

INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL

FORMULARIO DE SOLICITUD DE EJERCICIO DE DERECHOS

Reglamento General de Protección de Datos - RGPD

RESPONSABLE DEL TRATAMIENTO AL QUE DIRIGE LA SOLICITUD
Indique el responsable del tratamiento.

INTERESADO	
DNI	
APELLIDOS Y NOMBRE	
Por medio de la presente solicitud ejerce el derecho seleccionado, de conformidad con lo previsto en los artículos 15 a 22 del Reglamento (UE) 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 sus datos personales y a la libre circulación de estos datos	

REPRESENTANTE	
DNI	
APELLIDOS Y NOMBRE	

EJERCICIO DEL DERECHO		
Seleccione el derecho a ejercer:		
	ACCESO	El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la información establecida en el art. 15 del Reglamento (UE) 2016/679.
	RECTIFICACIÓN	El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional, de acuerdo a lo establecido en el art. 16 del Reglamento (UE) 2016/679.
	SUPRESIÓN	El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los dalos personales que le conciernan, el cual estará obligado a suprimir los datos personales cuando concurra alguna de las circunstancias previstas en el art. 17 del Reglamento (UE) 2016/679.
	OPOSICIÓN	El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento en base a lo establecido en el art. 21 del Reglamento (UE) 2016/679.
	LIMITACIÓN DEL TRATAMIENTO	El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones establecidas en el art. 18 del Reglamento (UE) 2016/679.
	PORTABILIDAD DE LOS DATOS	El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando se cumplan algunos de los requisitos establecidos en el art. 20 del Reglamento (UE) 2016/679.
	TRATAMIENTOS AUTOAMATIZADOS	El interesado tendrá derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles, que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, de acuerdo con lo previsto en el art. 22 del Reglamento (UE) 2016/679.

TEXTO DE LA SOLICITUD

MEDIO DE NOTIFICACIÓN		
	ELECTRÓNICO EMAIL	
	POSTAL (Cumplimente los datos de domicilio a efectos de notificación)	

DNI		**APELLIDOS Y NOMBRE**					
VÍA PÚBLICA							
NÚMERO		**ESCALERA**		**PISO**		**PUERTA**	
MUNICIPIO		**PROVINCIA**				**C.POSTAL**	

FIRMA							
EN		A		DE		DE	
Firma:							
Antes de firmar la solicitud debe leer la siguiente información sobre protección de datos personales:							
INFORMACIÓN SOBRE PROTECCIÓN DE DATOS PERSONALES							
Le informamos que el INSS como responsable del tratamiento, incluirá los datos personales que nos ha aportado, en el tratamiento de datos "Atención e Información Multicanal. Mejora de los servicios". Puede ejercer sus derechos en materia de Protección de Datos en cualquier momento. Para más información consulte la web: www.seg-social.es (apartado de protección de datos).							

MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES
INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL

Formulario descargable en el apartado de protección de datos de la intranet del INSS

ANEXO II

CARTEL

ZONA VIDEOVIGILADA

Cartel editable(PDF) en: www.aepd.es/es/areas-de-actuacion/videovigilancia

ZONA VIDEOVIGILADA

RESPONSABLE:

SUBDIRECCIÓN GENERAL DE RECURSOS HUMANOS Y MATERIALES DEL INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL.

PUEDE EJERCITAR SUS DERECHOS DE PROTECCIÓN DE DATOS ANTE:

DELEGADA DE PROTECCIÓN DE DATOS:
Calle Sagasta 13, sexta planta, 28004, Madrid.
Correo electrónico: delegado.protecciondatos@seg-social.es

MÁS INFORMACIÓN SOBRE EL TRATAMIENTO DE SUS DATOS PERSONALES:

Podrá obtener una información más amplia en materia de protección de datos personales en la web:
http://www.seg-social.es (apartado Protección de Datos: Seguridad Social Protección de datos)

ANEXO III

DECÁLOGO DE PROTECCIÓN DE DATOS PARA EL PERSONAL SANITARIO Y ADMINISTRATIVO DE LAS UNIDADES MÉDICAS DEL INSS

DECÁLOGO DE PROTECCIÓN DE DATOS PARA EL PERSONAL SANITARIO Y ADMINISTRATIVO DE LAS UNIDADES MÉDICAS DEL INSS

PROTECCIÓN DE DATOS INSS

1	Trata los datos personales de los interesados como querrías que tratasen los tuyos. Piensa en términos de protección de datos.
2	¿Estás seguro de que tienes que acceder a la historia clínica del Servicio Público de Salud? Consulta solo los informes o pruebas necesarios para la evaluación de la incapacidad laboral que estés valorando.
3	Recuerda: todos los accesos a la documentación clínica quedan registrados en el sistema y aplicativos (hora de acceso, documentación consultada, etc.). Los accesos son continuamente auditados.
4	Recuerda que no debes informar a terceros sobre los datos de salud de los interesados (salvo en caso de menores de edad o incapacitados).
5	Cuando salgas de la consulta o el despacho, bloquea la sesión de tu ordenador. Nunca facilites las claves de acceso, contraseñas, etc.
6	Evita enviar información con datos de salud por correo electrónico o por cualquier red pública inalámbrica de comunicación electrónica. En caso contrario, cifra la información.
7	Los documentos con datos personales deben ser destruidos conforme el procedimiento establecido en la Dirección provincial. Nunca los tires a la papelera.
8	Cuando finalices la consulta, cierra con llave los armarios o archivadores que contengan documentación clínica.
9	Nunca dejes las historias clínicas, y demás documentación con datos de salud a la vista de terceras personas o sin supervisión.
10	No crees tus propios ficheros o bases de datos referidos a la salud de los interesados. En caso de resultar necesario, debes obtener el consentimiento previo de la Dirección provincial

ANEXO IV

DECÁLOGO DE RECOMENDACIONES PARA COMPAGINAR EL TELETRABAJO Y LA PROTECCIÓN DE DATOS PERSONALES

DECÁLOGO DE RECOMENDACIONES PARA COMPAGINAR EL TELETRABAJO Y LA PROTECCIÓN DE DATOS PERSONALES	Seguridad Social Protección de datos INSS
1	El acceso a los Sistemas de Información de la Seguridad Social (SISS) solo se producirá por motivos laborales. Tan solo se accederá a los expedientes, ficheros o bases de datos que sean imprescindibles para el trámite administrativo que se esté realizando Está prohibido el uso para cualquier otro fin.
2	Recuerda que tienes la obligación de custodiar y no comunicar los elementos de identificación y autenticación que te han sido proporcionados para acceder a los sistemas informáticos (contraseñas, tafu, etc.), de forma que no puedan ser conocidos ni utilizados por terceros. Está prohibido que se utilicen accesos o credenciales de terceros, aunque dispongan de la autorización de su titular.
3	En caso de que sospeches que tu contraseña ha podido ser conocida fortuita o fraudulentamente por personas no autorizadas debes abrir una incidencia mediante la herramienta corporativa de registro de incidencias (REGISS) y proceder a su inmediata modificación.
4	En caso de que se te extravíe (o sufras el robo de) un soporte de identificación y autenticación (tafu, certificado digital, etc.), debes dirigirte a la Unidad expendedora (UPI o GISS) para proceder a la revocación de las credenciales asociadas y obtener unas nuevas.
5	El uso seguro del dispositivo electrónico es responsabilidad del usuario autorizado, por ello debes garantizar en todo momento que la información que se muestra en los mismos no sea visible a personas no autorizadas. Por ello debes bloquear la sesión o activar el salvapantallas cuando no estés en tu ordenador y apagar el ordenador y resto de dispositivos utilizados cuando finalice tu jornada.
6	Si el INSS te ha facilitado un dispositivo de movilidad para el teletrabajo, sigue las instrucciones facilitadas por la GISS, realizando un uso exclusivamente profesional de los portátiles o cualquier otro dispositivo tecnológico facilitado. No se recomienda, manipularlos o prestárselos a otras personas.
7	Si vas a utilizar un dispositivo personal para desempeñar tus funciones laborales, es de vital importancia que pongas a punto tu dispositivo para trabajar con él (Instala un antivirus para protegerlo de las posibles amenazas, actualiza el sistema operativo así como el resto de programas que tengas instalados en él a su última versión, crea una cuenta de usuario diferente en el dispositivo para separar tu espacio de trabajo personal del profesional). Salvaguarda la información (Realiza periódicamente copias de seguridad de la información que vayas generando en el dispositivo para no perderla, protege la información que tengas almacenada cifrando el disco duro, carpetas o ficheros que consideres que contienen información más crítica y confidencial).
8	En caso de que se te extravíe (o sufras el robo) de un dispositivo electrónico (tanto si es corporativo como si es personal) comunícalo a la mayor brevedad posible a la persona titular de tu Dirección provincial o de tu Subdirección general.
9	Revisa la configuración del router wifi de tu casa para asegurarte de que todas las medidas básicas de seguridad están establecidas. Evita conectarte a redes wifi abiertas y/o públicas, ya que no conoces qué medidas de seguridad, quién puede estar conectado a ella, ni cuáles son sus intenciones.
10	Activa tu sentido común y presta mucha atención a las noticias, mensajes, correos electrónicos o cualquier otra información que puedas recibir a través de los diferentes servicios que utilices para evitar ser víctimas de fraudes online o descargar malware aprovechándose de técnicas de engaño. No te creas cualquier noticia que recibas. Contrasta la información y no reenvíes mensajes participando en la difusión de noticias falsas y bulos. Si tienes **cualquier duda o problema, contacta con tu UPI o la GISS**. Adicionalmente, te recordamos que el Instituto Nacional de Ciberseguridad (INCIBE) tiene establecido el **teléfono 017,** línea de ayuda en ciberseguridad (llamada gratuita y confidencial) y la Oficina de Seguridad del Internauta: www.incibe.es/cibercovid19 y www.osi.es/es/cibercovid19

ANEXO V

INSTRUCCIONES PARA FIRMAR ELECTRÓNICAMENTE MINIMIZANDO DATOS

FIRMA ELECTRÓNICA DE DOCUEMENTOS EN FORMATO PDF

1.) Con minimización de datos (sin que aparezca número de DNI)

1. Busca en la Intranet del INSS la aplicación **"Mapa de Aplicaciones"** (la que es un librito al lado del mapa).
2. Selecciona **"Por orden alfabético"** y después en la letra E, la aplicación "**ePortafirmas Local"**.
3. Una vez que se te haya cargado el programa, donde pone **"Documentos",** clica en **"Examinar**" y buscas el documento en la carpeta o unidad de tu pc donde lo tengas guardado y lo seleccionas.
4. En el apartado de "**Datos huella de firma",** selecciona la hoja donde quieres firmar en la pestaña **"Página",** y a continuación clica sobre **"Refresh",** y te aparecerá la imagen de esa hoja en la pantalla lateral.
5. En la pantalla lateral donde se visualiza la hoja concreta que vas a firmar, clica sobre el rectángulo **"Huella de Firma"** y lo arrastras hasta situarlo en el lugar donde quieres que aparezca la firma, a continuación clica la pestaña **"Firmar"** y te saldrán los distintos certificados que tengas en tu pc (si vas a firmar con la TAFU debes tenerla introducida en el lector de tarjetas del teclado).
6. Por último, tras firmar te aparecerá el mensaje **"Documento firmado correctamente**", y debajo la pestaña **"Descargar",** clica sobre esta y ya lo guardas con el nombre y en la unidad que tú quieras.

Firmado electrónicamente por: LUIS VILAR MUÑOZ
En la fecha (hora GMT): 2020.03.03 y 13:19:52 CET

2.) Sin minimización de datos (si queremos que aparezca el número de DNI)

1. Busca en la columna lateral la pestaña **"Más herramientas".**
2. De las distintas opciones que te aparecen, selecciona **"Certificados".**
3. En el centro de la columna superior, selecciona **"Firmar digitalmente"**
4. En la parte del documento donde quieres que aparezca la firma, haz un recuadro arrastrando el ratón y manteniendo pinchado el botón principal.
5. A continuación te saldrá el certificado electrónico que tengas en el pc, pendrive, tafu… clica en **"Continuar",** te aparecerá la imagen de tu firma electrónica con tus datos, clica **"Firmar".**
6. Te aparecerá el desplegable de **"Guardar como",** pues ya elijes en que unidad lo vas a guardas y fin, ya tienes tu documento firmado digitalmente.