



En contestación a la información solicitada al amparo de la Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información pública y buen gobierno por
en el expediente **00001-00083231** sobre:

En el Centro Penitenciario de Valencia, el día 18 de octubre de 2023, desde Jefatura de Centro se llamó a los módulos residenciales y otros puestos singulares para que los trabajadores acudiesen a la Oficina de Personal a facilitar su huella dactilar.

Que según comentarios, esa huella se usará para establecer un sistema de control de horarios de los empleados públicos.

El artículo 12 de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, reconoce el derecho de todas las personas a acceder a la información pública, entendida, según el artículo 13 de esta misma Ley como “los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones”.

Por lo expuesto, SOLICITO se me informe de los siguientes conceptos:

- ***Órgano Colegiado o Unipersonal que dio esa Orden.***
- ***Se me facilite la propia Orden que obliga a facilitar al Centro Penitenciario la huella dactilar (dato biométrico). Dato personal denominado de “categoría especial”.***
- ***La base jurídica del tratamiento y, en su caso, circunstancia que levanta la prohibición para tratar categorías especiales de datos, según el artículo 9 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27/04/2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en lo sucesivo, RGPD), y que dan cobertura a dicho tipo de control de acceso.***
- ***Si no existen otras alternativas menos intrusivas y proporcionales. Motivos que justifiquen la necesidad y la proporcionalidad del uso de los datos biométricos para la finalidad perseguida.***
- ***Información sobre el cumplimiento del Reglamento General de Protección de Datos.***

- Información y copia del análisis de riesgos realizado (por ejemplo: robo de identidad).
- Información y copia de la Evaluación de Impacto relativa a la Protección de Datos, en caso de haberse realizado.
- Información sobre las medidas de seguridad implantadas en base al análisis de riesgos.
- El responsable del tratamiento, la identidad y los datos de contacto.
- Los datos de contacto del delegado de protección de datos.
- Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.
- Los intereses legítimos del responsable.
- Los destinatarios o las categorías de destinatarios de los datos personales.
- La intención del responsable de transferir esos datos personales.
- El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
- La existencia de decisiones automatizadas con esos datos, incluida la elaboración de perfiles.
- Descripción precisa del funcionamiento del instrumento utilizado para la captación de las huellas dactilares.
- Criterios utilizados para la codificación y el almacenamiento de la información captada (si los datos biométricos se almacenan en bruto o si son tratados de manera que sólo se almacena una plantilla biométrica).
- Medidas adoptadas para garantizar que no es posible la reutilización de los datos biométricos para otra finalidad.
- Si se está obligado a facilitar esa huella dactilar y las posibles consecuencias de no facilitar tal dato personal.
- Cómo ejercer los derechos de acceso, rectificación, supresión, portabilidad de los datos y la limitación u oposición a su tratamiento.

En contestación de las cuestiones planteadas, se incluye a continuación la descripción del tratamiento de datos sobre el que se pregunta: Gestión de acceso y control horario en los centros penitenciarios. En dicha descripción, en cumplimiento del artículo 31 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos y garantía de derechos digitales, se da respuesta a parte de las solicitudes que anteriormente se enumeran puesto que algunas exigirían elaborar informes específicos al efecto o facilitar información que, por motivos de seguridad del sistema y de las propias personas implicadas, no puede proporcionarse.

Igualmente, se encuentra disponible en el Registro de Actividades de Tratamiento del Ministerio del Interior y publicado en el Portal de Transparencia.

Responsable del tratamiento	Director de cada centro penitenciario (DIR3 E04946301) Disponible en página web https://www.institucionpenitenciaria.es o a través del DPD. Correo electrónico: dpd_instpenit@dgip.mir.es
Corresponsable	No existe. Se trata de una responsabilidad delegada del titular de la Secretaría General de Instituciones Penitenciarias.
Delegado de Protección de Datos	Delegado de Protección de Datos de la Secretaría General de Instituciones Penitenciarias y de la Entidad Estatal de Derecho Público de Trabajo Penitenciario y Formación para el Empleo (DIR3E04946301) C/ Alcalá 38, Madrid 28014. Correo electrónico: dpd_instpenit@dgip.mir.es
Fines del Tratamiento	Acceso controlado a los centros penitenciarios por personal habilitado para ello de acuerdo con el horario asignado.
Base legal (legitimación)	Reglamento Europeo 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, LO 3/2018, de 5 de diciembre, de protección de datos y garantía de derechos digitales; normas legales y reglamentarias reguladoras del empleo público. Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria.
Categorías de interesados	Personal dependiente de la Secretaría General de Instituciones Penitenciarias destinada en los centros penitenciarios.
Categorías de datos personales	Nombre y apellidos, DNI, número de registro personal, datos biométricos (plantillas sin almacenaje).
Categorías de destinatarios	No están previstas las cesiones excepto en aplicación específica de la normativa.
Transferencias internacionales	No está prevista la cesión de datos internacional.
Plazo de supresión	Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Será de aplicación lo dispuesto en la normativa de archivos y documentación.
Medidas de seguridad y organizativas de seguridad	Entre otras, el acceso a los equipos informáticos se realiza con usuario y contraseña; a las aplicaciones informáticas sólo accede personal previamente autorizado y a las aplicaciones de las que se es responsable se accede con usuario y contraseña; en su caso, encriptación y cifrado.

Se solicita igualmente copia del Análisis de Riesgos llevado a cabo y de la correspondiente Evaluación de Impacto. En relación con estos documentos, por su contenido intrínseco, su publicidad completa y generalizada supone un riesgo para la propia consistencia e integridad del tratamiento de datos que en cada caso nos ocupe. Ello en la medida en que se facilitaría el ataque a los sistemas de tratamiento aumentando su vulnerabilidad. Sin embargo, en aplicación del artículo 16 de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, sobre acceso parcial, se participa parte de su contenido en contestación a las cuestiones planteadas.

En primer lugar, sobre la necesidad del tratamiento y su proporcionalidad en comparación con otros sistemas de control del acceso a centros penitenciarios, la implementación de sistemas como el que nos ocupa se relaciona directamente con la misión pública de garantizar la seguridad en los centros penitenciarios recogido en el artículo 1 de la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria. Ello no sólo en cuanto a las personas privadas de libertad, sino también en cuanto a los profesionales. En este sentido, no existe otro sistema igual de eficaz y menos intrusivo en relación con la finalidad señalada que, por ejemplo, permita ataques de malware, interceptación de señales RFID, pueda evitar pérdidas de tarjetas identificativas o robos intencionados de las mismas. Se ha de señalar que, por la especificidad de sus funciones, las personas que trabajan en los centros gozan de otras medidas especiales de protección que pretenden elevar las garantías de su seguridad.

En segundo lugar, no obstante lo anterior y siendo conscientes de la relevancia de los tratamientos de datos que llevamos a cabo, los mismos se desarrollan tratando de adaptar las medidas de seguridad adecuadas para cada caso. En concreto para el tratamiento Gestión de acceso y control horario en los centros penitenciarios que da lugar a este expediente (CP Valencia), se trata de un tratamiento en el que no se prevén transferencias al exterior, sin generación de tratamientos automatizados o creación de perfiles, sin almacenaje de huellas dactilares (patrón mínimo que se se ha obtenido en el proceso) y con un tiempo de conservación estrictamente limitado al tiempo activo en el centro de referencia. Sobre el funcionamiento específico, el instrumento utilizado es un sensor óptico que emplea cuatro tecnologías y métodos para asegurar que los terminales no detecten huellas falsas de papel, plástico, goma, silicona, gelatina, etc. Una vez detecta la presencia de un dedo vivo inicia el proceso automáticamente, sin la presencia de un servidor o controladora. Todas las reglas de control de acceso se procesan en la propia placa del terminal, permaneciendo operativo.

Finalmente, no se trata de un tratamiento de datos basado en el consentimiento sin que puedan ni deban preverse con carácter generalizado las consencuencias de obstaculizar su implementación y sin que exista documento publico específico sobre dicha cuestión.

Teniendo en cuenta lo expuesto, la petición formulada queda parcialmente fuera de lo establecido en el artículo 7.a), 8 y 13 de la LTAIPBG, y asimismo le serían aplicables entre otras, las limitaciones de exclusión establecidas en los artículos 14 a) y d) y 18.1 y 2 de la citada Ley, procede entender la INADMISIÓN de la solicitud requerida y LIMITADA de conformidad con los perjuicios aludidos

Contra la presente resolución, que pone fin a la vía administrativa, podrá interponerse recurso contencioso-administrativo ante los Juzgados Centrales de lo Contencioso-administrativo, en el plazo de dos meses o, previa y potestativamente, reclamación ante el Consejo de Transparencia y Buen Gobierno en el plazo de un mes; en ambos casos, el plazo se contará desde el día siguiente al de la notificación de la presente resolución.

EL SECRETARIO GENERAL DE
INSTITUCIONES PENITENCIARIAS
Ángel Luis Ortiz González