



## **POLÍTICA DE PRIVACIDAD DEL SISTEMA INTERNO DE INFORMACIÓN**

### **1. OBJETO**

El objetivo de la presente Política de Privacidad del Sistema Interno de Información de JBC es informar del tratamiento de los datos que se llevará a cabo para la gestión y tramitación de las comunicaciones presentadas a través del mismo.

### **2. RESPONSABLE DEL TRATAMIENTO DE LOS DATOS**

El responsable del tratamiento de los datos es

**JBC Soldering SL** NIF: B65356172

Dirección postal: **C/ Ramon y Cajal, 3 08750 Molins de Rei (España)**

Correo electrónico: [jbctools@jbctools.com](mailto:jbctools@jbctools.com)

### **3. PROCEDENCIA DE LOS DATOS PERSONALES**

En el Sistema Interno de Información se tratará información personal del informante y del afectado, así como de terceras personas involucradas en los hechos objeto de información o referentes a consultas realizadas.

Dichos datos podrán ser facilitados: (a) por el informante o interesado (b) por cualquiera de las demás personas involucradas en la investigación, respecto de las restantes, o (c) por JBC, por su condición de empleadora de los mismos.

### **4. LICITUD, FINALIDAD Y LEGITIMACIÓN**

Conforme al artículo 30 de la Ley 2/2023, y de acuerdo siempre con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se consideran lícitos los tratamientos de datos personales que sean necesarios para la aplicación de dicha ley, así como el tratamiento de datos personales de comunicaciones internas, los de canales de comunicación externa, los derivados de u una revelación pública y los de categorías especiales de datos personales por razones de un interés público esencial.

Los datos personales que sean recabados en el Sistema Interno de Información serán tratados con la exclusiva finalidad de tramitar las comunicaciones que se reciban y, si procede, investigar la realidad de los hechos o conductas informadas, preservando siempre la identidad del informante y garantizando la protección adecuada frente a las represalias que puedan sufrir las personas físicas informantes, el fortalecimiento de la cultura de la información, de las infraestructuras de integridad de las organizaciones y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público.

Finalmente, en algunos casos los datos personales también podrán ser tratados para dar cumplimiento a determinadas obligaciones legales que sean de aplicación a la compañía. En estos casos, y en la medida de lo posible, se informará de ello y de la norma que lo impone.

## **5. TIEMPO DE CONSERVACIÓN DE SUS DATOS**

Los datos de quien aporte la información, del afectado, de miembros de JBC y de terceros (Proveedores, Asociados, etc.) que participen en la investigación de una información, serán conservados en el sistema interno de información inicialmente durante el tiempo imprescindible para (a) decidir sobre la procedencia de iniciar una investigación sobre los hechos informados y, en su caso, (b) durante el tiempo en que se desarrolle –en el seno de la organización- la pertinente investigación.

Si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos.

Los datos que sean objeto de tratamiento se conservarán únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.

Si se acreditara que la información facilitada o parte de ella no es veraz, se procederá a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, se procederá a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema.

Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

Los empleados y terceros deberán ser informados acerca del tratamiento de datos personales en el marco de los Sistemas de información.

En ningún caso podrán conservarse datos por un periodo superior a diez (10) años.

## **6. LIMITACIÓN AL ACCESO DE LOS DATOS ¿A QUÉ DESTINATARIOS SE COMUNICARÁN SUS DATOS?**

El acceso a los datos personales contenidos en el Sistema Interno de Información quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a:

- a) El Responsable del Sistema y el Responsable de Prevención de Riesgos Penales.
- b) El Responsable de Recursos Humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.

c) El Responsable del Asesoramiento legal externo o Responsable de los servicios jurídicos de la entidad u organismo, si lo hubiera, y si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.

d) Los encargados del tratamiento que eventualmente se designen.

e) El delegado de protección de datos, o responsable de protección de datos.

Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones a las que se refiere el artículo 2, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la ley. En caso de que sea necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que procedan, los datos podrán ser comunicados a aquellos terceros a los que esté legalmente obligado a facilitarlos, tales como Organismos Públicos, Jueces y Tribunales o Cuerpos y Fuerzas de Seguridad.

Asimismo, JBC cuenta con la colaboración de terceros proveedores de servicios que pueden tener acceso a sus datos personales y que tratarán los referidos datos en su nombre y por su cuenta.

En relación con lo anterior se pone de manifiesto que JBC sigue unos criterios estrictos de selección de proveedores de servicios con el fin de dar cumplimiento a sus obligaciones en materia de protección de datos y se compromete a suscribir con ellos el correspondiente contrato de tratamiento de datos mediante el que les impondrá, entre otras, las siguientes obligaciones: aplicar medidas técnicas y organizativas apropiadas; tratar los datos solo para las finalidades pactadas y atendiendo únicamente a las instrucciones documentadas de JBC y suprimir o devolver los datos una vez finalice la prestación de los servicios.

En concreto, JBC podrá contratar la prestación de servicios por parte de terceros proveedores que desempeñan su actividad, a título enunciativo y no limitativo, en los siguientes sectores: asesoramiento jurídico, empresas de servicios profesionales multidisciplinarios, o empresas proveedoras de servicios tecnológicos o informáticos.

## **7. EJERCICIO DE DERECHOS**

- a) Las personas cuyos datos personales puedan llegar a ser tratados en el marco y contexto del Sistema Interno de Información tienen derecho a recibir la información contenida en el presente anexo, en cumplimiento de lo dispuesto en el artículo 13 del RGPD. Así, tendrán derecho a obtener confirmación sobre si en JBC se están tratando sus datos personales o no –en el marco de la gestión del Sistema Interno de Información-, así como a acceder, rectificar, limitar el uso de sus datos, o en su caso, solicitar su supresión, en los términos legalmente establecidos, cuando, entre otros motivos, los datos ya no sean necesarios para la gestión del Sistema Interno de Información.
- b) En determinadas circunstancias, a oponerse al tratamiento de sus datos personales.

El contacto para cuestiones relativas a la Protección de datos es [jbctools@jbctools.com](mailto:jbctools@jbctools.com) , a quien tanto informantes como afectados por las informaciones se podrán dirigir para consultar cualquier cuestión relativa, estrictamente, al tratamiento de sus datos personales, así como para el ejercicio de sus legítimos derechos en materia de Privacidad.

También podrá reclamar ante la Agencia Española de Protección de Datos (como tal Autoridad de Control competente en materia de Protección de datos), especialmente cuando no haya obtenido satisfacción en el ejercicio de sus derechos a través del mencionado email, mediante escrito dirigido a Agencia Española de Protección de Datos C/ Jorge Juan, 6 28001-Madrid o a través de la web <https://www.aepd.es>

## **8. PRINCIPIO DE PROPORCIONALIDAD Y MINIMIZACIÓN DE DATOS**

- ✓ Los datos personales recabados en el marco del Sistema Interno de Información: se limitarán a los estricta y objetivamente necesarios para tramitar las consultas, las informaciones y, si procede, comprobar la realidad de los hechos comunicados;
- ✓ Serán tratados en todo momento de conformidad con la normativa de protección de datos aplicable, para fines legítimos y específicos en relación con la investigación que pueda surgir como consecuencia de la comunicación.
- ✓ Serán adecuados y no excesivos en relación con las citadas finalidades.

## **9. MEDIDAS DE SEGURIDAD Y CONFIDENCIALIDAD**

JBC se asegurará de que se adopten todas las medidas técnicas y organizativas necesarias para preservar la seguridad de los datos recabados al objeto de protegerlos de divulgaciones o accesos no autorizados.

A estos efectos, JBC ha adoptado medidas apropiadas para garantizar la confidencialidad de todos los datos y se asegurará de que los datos relativos a la identidad del informante no sean divulgados al afectado durante la investigación, respetando en todo caso los derechos fundamentales de la persona, sin perjuicio de las acciones que, en su caso, puedan adoptar las autoridades judiciales competentes.

Las personas informantes tendrán derecho a medidas de protección y de apoyo que la Ley 2/2023 otorga. Se prohíben expresamente los actos constitutivos de represalia tales como suspensión del contrato de trabajo, despido o extinción de la relación laboral; daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo, evaluación o referencias negativas, inclusión en listas negras, denegación o anulación de licencia o permiso, denegación de formación y discriminación.