Anexo V: TRATAMIENTO DE DATOS PERSONALES

COLECTIVOS Y DATOS TRATADOS

Las categorías de personas interesadas cuyos datos serán tratados por la organización ENCARGADA DE TRATAMIENTO son las siguientes:

- Empresas/agentes/organizaciones tanto públicas como privadas, relacionadas directa o indirectamente con el producto cultural de Pamplona.

Para la ejecución del contrato objeto de este pliego la adjudicataria puede acceder a los siguientes tipos de datos:

- Datos identificativos (nombre y apellidos).
- Datos de detalles de empleo (profesión, puesto de trabajo).
- Datos de información comercial (actividades o negocios).

DERECHO DE INFORMACIÓN. La organización encargada, en el momento de la recogida de los datos, debe facilitar la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos.

MEDIDAS DE SEGURIDAD

La entidad adjudicataria deberá ofrecer las garantías suficientes para aplicar las medidas técnicas y organizativas que aseguren que el tratamiento de los datos de carácter personal del que es responsable el Ayuntamiento de Pamplona es conforme a los requisitos de la normativa de protección de datos y garantiza la protección de los derechos de las personas interesadas para lo que deberá implementar al menos las siguientes medidas de seguridad:

- Definir, y documentar, las funciones y obligaciones de las diferentes personas usuarias, o perfiles de usuarios, difundirlas entre el personal, así como las consecuencias de su incumplimiento.
- Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- Disponer de un procedimiento de notificación, registro y gestión de incidencias y violaciones de seguridad, conforme a lo previsto en el RGPD que recoja: tipo de incidencia/violación, momento de su detección, persona que la notifica, efectos y medidas correctoras. Cualquier incidencia que afecte a la integridad, confidencialidad, autenticidad y disponibilidad del tratamiento de los datos de carácter personal llevada a cabo por la organización encargada de tratamiento será comunicada de inmediato al responsable del tratamiento.
- Disponer de un procedimiento para la gestión de los derechos de acceso, rectificación, supresión, oposición y limitación del tratamiento como encargados de tratamiento.

- Establecer métodos de cifrado y seudoanonimización en caso de gestión de soportes fuera de los locales de la organización responsable o encargada de tratamiento.
- Incluir sistemas de auditoría y registro (logs de acceso) en las aplicaciones que tratan datos de categorías especiales.
- No debe utilizar herramientas que no ofrezcan garantías del cumplimiento de la normativa de protección de datos.
- Todos los equipos que se conecten a sistemas o traten datos personales del Ayuntamiento deben disponer al menos de:
  - antivirus activado y actualizado con periodicidad diaria
  - Firewall.
- Se debe establecer un control de acceso según las funciones asignadas a las personas trabajadoras, que eviten el acceso a datos o recursos distintos de los autorizados. Las mismas condiciones deberán existir para el personal ajeno con acceso datos personales.
- Las credenciales de acceso identificarán a los usuarios de manera inequívoca y personalizada. En caso de usuarios externos, se permitirá el acceso a los datos personales a usuarios con los permisos adecuados mediante conexiones Red Privad Virtual (VPN) o similares que garanticen la confidencialidad de la información. Dichos permisos de acceso sólo podrán concederse por personal autorizado.
- La organización encargada de tratamiento deberá disponer de un sistema de identificación y autenticación personalizada, los usuarios y contraseñas, deberán almacenarse de forma ininteligible y cambiarse periódicamente al menos de forma anual, disponiendo de un límite de intentos reiterados de acceso no autorizado.
- Los dispositivos portátiles dispondrán de una contraseña a nivel de BIOS.
- Se dispondrá de sistemas de control de acceso físico a la ubicación de los sistemas de información mediante llave, tarjeta magnética o similar, código de acceso, la documentación en papel con datos especialmente protegidos deberá estar custodiada en armarios, cajones, etc., con llave, ubicados en áreas con acceso protegido mediante puertas con llave.
- La organización encargada del tratamiento dispondrá de procedimientos documentados de copias de respaldo y recuperación de los datos personales que trate por cuenta del Responsable. El acceso a los soportes de copia se encontrará restringido, evitando accesos no autorizados.
  Semestralmente se verificará el proceso de copias de seguridad en el caso de que contengan información de la que sea responsable el Ayuntamiento de Pamplona.
  Las copias de respaldo se conservarán en lugar diferente del que se encuentren los equipos sobre los que se hace la copia.
- Los documentos en formato papel deben archivarse en lugares que impidan el acceso a personas no autorizadas. Deberá estar custodiada en armarios, cajones etc., con mecanismos que impidan su apertura.

- Igualmente,
  durante la tramitación o traslado de documentos, la persona a cargo de los mismos debe custodiarla para evitar accesos no autorizados. El traslado se realizará con mecanismos que impidan el acceso o manipulación u obstaculicen su apertura. Los soportes deberán estar etiquetados mediante sistemas únicamente comprensibles a nivel interno de la organización.