III. OTRAS DISPOSICIONES

MINISTERIO DE CULTURA Y DEPORTE

19756 *Resolución de 11 de septiembre de 2023, de la Subsecretaría, por la que se publica la Adenda al Convenio con la Sociedad Estatal Correos y Telégrafos, SA, S.M.E., para la facilitación y gestión de los medios de pago de las ayudas del «Bono Cultural Joven 2023».*

Por Orden CUD/496/2023, de 18 de mayo, («Boletín Oficial del Estado» núm. 119, de 18 de mayo de 2023) se convocó el procedimiento de concurrencia para la selección de una entidad colaboradora para la facilitación y gestión de los medios de pago del programa de ayudas «Bono Cultural Joven 2023».

Una vez tramitado el correspondiente procedimiento, previsto en la citada Orden CUD/496/2023, de 18 de mayo, se dictó Resolución de la Subsecretaria de Cultura y Deporte, de fecha 19 de junio de 2023, por la que se seleccionó a la Sociedad Estatal de Correos y Telégrafos, SA, S.M.E. como entidad colaboradora que se encarga de la facilitación y gestión de los medios de pago de las ayudas del Bono Cultural Joven, convocadas en 2023. Esta resolución fue publicada en la sede electrónica del Ministerio de Cultura y Deporte, conforme a lo establecido en el artículo 12 de la referida Orden CUD/496/2023, de 18 de mayo.

Igualmente la mencionada resolución ordenaba la formalización de un convenio de colaboración entre el Ministerio de Cultura y Deporte y la entidad seleccionada, que fue finalmente suscrito en fecha 26 de julio de 2023, inscrito en el Registro Electrónico estatal de Órganos e Instrumentos de Cooperación del sector público estatal (REOICO) y publicado en el «Boletín Oficial del Estado» (BOE) mediante Resolución de 31 de julio de la Subsecretaría, en fecha 7 de agosto de 2023.

Con posterioridad a la celebración del mencionado convenio, ha sido preciso ampliar su contenido en materia de protección de datos personales, mediante la tramitación de una adenda al mismo, que cuenta con informe favorable de la Abogacía del Estado destacada en el Ministerio de Cultura y Deporte, de fecha 7 de septiembre de 2023.

Una vez perfeccionada la adenda al convenio de colaboración con la firma de ambas partes en fecha 8 de septiembre de 2023 y de conformidad con lo dispuesto en la cláusula décima del citado convenio, dispongo:

Única.

Ordenar la inscripción de la adenda al convenio de colaboración en el Registro Electrónico estatal de Órganos e Instrumentos de Cooperación del sector público estatal, previsto en el artículo 48.8 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, así como su publicación en el «Boletín Oficial del Estado».

Esta resolución no pone fin a la vía administrativa y contra la misma se podrá interponer recurso de alzada ante la persona titular del Ministerio de Cultura y Deporte, en el plazo de un mes a contar desde el día siguiente a la publicación en la sede electrónica, de conformidad con lo establecido en los artículos 121 y 122 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Madrid, 11 de septiembre de 2023.–La Subsecretaria de Cultura y Deporte, María Pérez Sánchez-Laulhé.

cve: BOE-A-2023-19756
Verificable en https://www.boe.es

ADENDA AL CONVENIO DE COLABORACIÓN ENTRE EL MINISTERIO DE CULTURA Y DEPORTE A TRAVÉS DE LA SUBSECRETARÍA DE CULTURA Y DEPORTE Y SOCIEDAD ESTATAL CORREOS Y TELÉGRAFOS, SA, S.M.E. PARA LA FACILITACIÓN Y GESTIÓN DE LOS MEDIOS DE PAGO DE LAS AYUDAS DEL «BONO CULTURAL JOVEN 2023», DE 26 DE JULIO DE 2023

A 8 de septiembre de 2023.

REUNIDOS

De una parte, doña María Pérez Sánchez-Laulhé, Subsecretaria del Ministerio de Cultura y Deporte, nombrada mediante Real Decreto 108/2023, de 14 de febrero (BOE núm. 39, de 15 de febrero de 2023), conforme a las atribuciones que le confiere el artículo 63 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el artículo 6 del Real Decreto 509/2020, de 5 de mayo, por el que se desarrolla la estructura orgánica básica del Ministerio de Cultura y Deporte y el apartado Undécimo h) de la Orden CUD/990/2020, de 16 de octubre, sobre fijación de límites para la administración de determinados créditos para gastos y de delegación de competencias.

Y de otra parte, la Sociedad Estatal Correos y Telégrafos, SA, S.M.E., con domicilio a los efectos en Madrid, calle Conde de Peñalver 19, 28006, NIF: A83052407 y representada legalmente por doña Leire Díez de Castro, con DNI ***8531**, actuando en su condición de Directora de Filatelia, Estudios y Futuro, mancomunadamente con doña Nuria Lera Hervás, con DNI ***5857** actuando en su condición de Directora de Relaciones Institucionales, en virtud de las facultades emanadas de los poderes conferidos en escritura otorgada ante el Notario de Madrid, don Juan Kutz Azqueta, a 28 de febrero de 2023, con el número 358 de su protocolo.

Todos ellos se denominarán «las Partes».

Actuando las Partes en razón de sus respectivas competencias y reconociéndose poderes y facultades para formalizar la presente adenda al convenio de colaboración, a cuyo efecto,

EXPONEN

1. Que la Resolución de la Subsecretaria de Cultura y Deporte, de 19 de junio de 2023, por la que se selecciona la entidad colaboradora que se encargará de la facilitación y gestión de los medios de pago del programa de ayudas «Bono Cultural Joven 2023», en cumplimiento de la Orden CUD/496/2023, de 18 de mayo, se seleccionó como entidad colaboradora para el fin mencionado a la Sociedad Estatal Correos y Telégrafos, SA, S.M.E.

2. Que, una vez dictada la citada resolución de selección y según lo establecido en la Orden CUD/496/2023, se procedió, en fecha 26 de julio de 2023, a la firma entre la Subsecretaría de Cultura y Deporte y la Sociedad Estatal Correos y Telégrafos, SA, S.M.E. del correspondiente convenio de colaboración.

3. Que en la cláusula octava del Convenio de Colaboración se regula el régimen aplicable en materia de protección de datos entre las Partes.

4. Que, con la presente adenda, se pretende modificar al amparo de lo dispuesto en la cláusula undécima del convenio de colaboración firmado por las Partes el 26 de julio de 2023, de conformidad con las siguientes

cve: BOE-A-2023-19756
Verificable en https://www.boe.es

CLÁUSULAS

Primera. *Modificación del convenio.*

1.1 Las Partes acuerdan modificar el apartado c) de la cláusula octava relativa a la adopción de medidas de índole técnica y organizativas apropiadas en los siguientes términos:

> «Adoptar las medidas de índole técnica y organizativas apropiadas que garanticen un nivel de seguridad de los datos de carácter personal adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.»

1.2 Las Partes acuerdan modificar el apartado d) de la cláusula octava relativa a los subencargados en el tratamiento de datos en los siguientes términos:

> «d) En caso de recurrir a otro encargado del tratamiento, respetará las condiciones indicadas en los apartados 2 y 4 del artículo 28 del RGPD.
>
> A estos efectos, el Ministerio de Cultura y Deporte autoriza a la Sociedad Estatal Correos y Telégrafos, SA, S.M.E. a recurrir, como subencargado del tratamiento, a Bnext Electronic Issuer, E.D.E., SL, con NIF: B-88463534 y con domicilio en calle Zurbano 71, Madrid, 28010 (en adelante, "BNEXT"), o a cualquiera que la sustituya previa conformidad del Ministerio de Cultura y Deporte, en el desarrollo de las prestaciones que la Sociedad Estatal Correos y Telégrafos, SA, S.M.E. tiene encomendadas para el cumplimiento del objeto de la colaboración, de conformidad con lo dispuesto en 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, en lo que afecta a la subcontratación. Asimismo, el Ministerio de Cultura y Deporte autoriza a Bnext Electronic Issuer, E.D.E., SL, o a cualquiera que la sustituya a subcontratar en las condiciones y requisitos formales indicados en este párrafo.
>
> BNEXT, como entidad que colabora en la emisión de las tarjetas Correos Prepago, recibirá de forma segura, a través de la plataforma de la FNMT-RCM mediante APIs, los datos personales mínimos necesarios con el objetivo de emitir las tarjetas de las personas beneficiarias de las ayudas. Dichos datos serán veraces y se encontrarán en todo momento actualizados.
>
> Asimismo y para la ejecución del programa de ayudas "Bono Cultural Joven 2023", el Ministerio de Cultura y Deporte autoriza a la Sociedad Estatal Correos y Telégrafos, SA, S.M.E. a comunicar a BNEXT, en calidad de Entidad de Pagos y Dinero Electrónico, los datos personales que sean necesarios para las finalidades relativas al cumplimiento de la Ley 21/2011, de 26 de julio, de dinero electrónico, así como para la Prevención del Blanqueo de Capitales y Financiación del Terrorismo o Fraude sobre los medios de pago y la aplicación de las medidas de diligencia relativas a la identificación formal de los beneficiarios de conformidad con los artículos 8 y 13 de la Ley 10/2010, de 28 de abril, de prevención del Blanqueo de Capitales y Financiación del Terrorismo y el Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la citada Ley.»

cve: BOE-A-2023-19756
Verificable en https://www.boe.es

1.3 Las partes acuerdan incorporar un anexo relativo al tratamiento de datos personales en los siguientes términos:

«a) Categorización Esquema Nacional de Seguridad (ENS).

De conformidad con lo dispuesto en el artículo 38 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), el Ministerio de Cultura y Deporte ha catalogado el servicio-sistema de la siguiente forma:

	D	I	C	A	T
Servicio de Bono Cultural Joven.	B	N/A	N/A	N/A	N/A
Información de Datos personales de los jóvenes beneficiarios (identidad, residencia legal).	N/A	B	B	B	B
Información de Datos de las entidades adheridas.	N/A	B	B	B	B
Información de la gestión de las ayudas del bono cultural joven.	N/A	M	B	M	B
Categorización máxima.	B	M	B	M	B

En virtud de la anterior categorización, son de aplicación las medidas de seguridad del anexo II del ENS.

b) Instrucciones iniciales de coordinación del responsable del tratamiento de los datos personales del Bono Cultural Joven 2023 en relación con el artículo 28 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 los datos personales y a la libre circulación de estos datos (RGPD) y los acuerdos previos convenidos con los encargados.

Descripción general del tratamiento de Datos Personales a efectuar.

El tratamiento consistirá en la facilitación y gestión de los medios de pagos de las ayudas del Bono Cultural Joven 2023 a las personas beneficiarias, incluyendo la gestión de la plataforma y aplicaciones informáticas para la puesta en marcha y ejecución del Bono Cultural Joven 2023, emisión, administración y gestión de la prestación de las Tarjetas Correos Prepago para el Bono Cultural Joven 2023 así como su distribución a los Beneficiarios, call center para la atención a Beneficiarios sobre la facilitación y gestión de los medios de pago.

Igualmente, la Sociedad Estatal Correos y Telégrafos, SA, S.M.E. se encargará de gestionar la autorización de altas y bajas de los terminales de puntos de venta (TPV) y FUC de las entidades adheridas al programa, a los efectos de aceptar pagos de los medios de pago emitidos.

Colectivo y datos tratados.

1. Personas beneficiarias de las ayudas del Bono Cultural Joven 2023.

Ciudadanos que cumplen 18 años en 2023: Nombre y apellidos, documento de Identificación (DNI o NIE), fecha de nacimiento, sexo, nacionalidad, domicilio legal, número de teléfono, correo electrónico, identificador de tarjeta (cardholderID), fecha de alta y fecha de baja de la tarjeta; estado de la tarjeta (abierta, activa, bloqueada, etc.); tipo de tarjeta (física o virtual), movimientos de la tarjeta.

Representantes legales de los anteriores: Nombre y apellidos, NIF o documento legal equivalente, número de teléfono y correo electrónico.

cve: BOE-A-2023-19756
Verificable en https://www.boe.es

2. Entidades adheridas como personas físicas (autónomos) y representantes de personas jurídicas.

Nombre y apellidos del interesado/a, del representante legal o razón social de la persona jurídica que actúa como representante, cuando proceda, NIF de la entidad, documentación de identificación del representante, domicilio fiscal del interesado/a, domicilio a efectos de notificaciones, correo electrónico de entidad y representante, número de teléfono, fecha de adhesión y, en caso, renuncia al programa, epígrafe IAE de la actividad principal; otros epígrafes IAE de actividades secundarias; código CNAE de la actividad principal; otros códigos CNAE de actividades secundaria; datos de localización de la sede de la entidad (códigos oficiales –predefinidos y cerrados– de municipio, provincia y comunidad autónoma); tipo de entidad (Internet, gran superficie; especializado…), identificador del comercio dentro de la entidad (identificador univoco asignado al comercio, MerchanID); denominación comercio; identificador del TPV (Terminal ID); categoría del TPV (productos en soporte físico; contenido digital o en línea; y artes en vivo, patrimonio cultural y artes audiovisuales); fecha de alta y fecha de baja del TPV, datos de ubicación del comercio (códigos oficiales –predefinidos y cerrados- de municipio, provincia y comunidad autónoma), cuantía de la transacción comercial (de compra o devolución, mAmount1); identificador de la operación; código de producto, según las categorías previstas en el artículo 8 del Real Decreto 191/2023, de 21 de marzo:

– Artes en vivo, patrimonio cultural y artes audiovisuales: patrimonio cultural (museos; monumentos; bibliotecas; otros); escénicos o musicales (teatro; danza; zarzuela; ópera; circo; toros; conciertos); cine.
– Productos en soporte físico (libros; prensa o revistas; partituras; música; videos, videojuegos, otros).
– Contenido digital o en línea: (suscripciones plataformas (libros; prensa; música, audiovisual; videojuegos); compra de soportes digitales (libros, música, videos, videojuegos, otros).

En el caso de las personas beneficiarias de la ayuda del Bono Cultural Joven, se evitará, en la medida de lo posible, el tratamiento de datos personales de categoría especial por parte del Responsable del Tratamiento. En el caso de que lo anterior no fuera posible, se aportarían nuevas instrucciones por parte del Responsable del Tratamiento con el fin de reforzar las garantías y mitigar cualquier riesgo para los derechos y libertades de las personas afectadas. La comunicación se realizaría, cuando proceda, conforme a lo dispuesto en el artículo 18.1.a) de la Ley 12/2009, de 30 de octubre, reguladora del derecho de asilo y de la protección subsidiaria o con la protección temporal definida en el Real Decreto 1325/2003, de 24 de octubre, por el que se aprueba el Reglamento sobre régimen de protección temporal en caso de afluencia masiva de personas desplazadas.

El encargado tratará los datos personales que sean estrictamente necesarios para cumplir con las obligaciones y actividades derivadas del encargo, en cumplimiento del principio de minimización definido en el RGPD y el artículo 15.4.b) del Real Decreto 191/2023, de 21 de marzo siguiendo, en todo caso, las instrucciones ofrecidas por el Ministerio de Cultura y Deporte en calidad de Responsable del Tratamiento. En caso necesario, el Responsable del Tratamiento determinará los datos concretos que pueden tratar el Encargado del Tratamiento en las comunicaciones necesarias entre ellas para la ejecución del Bono Cultural Joven.

Medidas adicionales.

Las medidas de seguridad implantadas para el tratamiento podrán ser objeto de modificación, supresión y/o novación en aras a dar cumplimiento a las

cve: BOE-A-2023-19756
Verificable en https://www.boe.es

exigencias que impone el Reglamento General de Protección de Datos (RGPD) y resto de normativa vigente. A estos efectos, el Ministerio de Cultura y Deporte notificará por escrito a la Sociedad Estatal Correos y Telégrafos, SA, S.M.E. cualquier modificación, supresión y/o novación sobre las medidas de seguridad a implementar. Específicamente deberán seguirse las establecidas en el artículo 32.1 del RGPD, la Disposición Adicional primera en su punto 2 de la LOPDGDD, las que figuran en los instrumentos de colaboración de las entidades colaboradoras en la gestión del programa así como las siguientes medidas de seguridad tanto técnicas como organizativas y de cumplimiento adicionales, sin perjuicio de la existencia de otras medidas de seguridad complementarias para asegurar el cumplimiento legal en materia de protección de datos personales o Esquema Nacional de Seguridad (ENS), en el nivel que se ha determinado y contemplado en el presente anexo:

a) La conservación de los datos personales será un elemento de tratamiento de la Sociedad Estatal Correos y Telégrafos, SA, S.M.E. y se hará en servidores locales con backups diarios siempre en servidores diferentes y aislados para garantizar la integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento. En el caso de no poder gestionarse en servidores locales, los servidores estarán ubicados en la UE o en el Espacio Económico Europeo (EEE). La finalidad primordial es evitar el daño por ransomware y cualquier otro tipo de ataque de ciberseguridad.

b) No se realizarán transferencias internacionales de ningún tipo. En caso de servicios de computación en la nube y subcontratación por parte del encargado, se exigirá que pongan en conocimiento del responsable transferencias internacionales de datos y, en caso afirmativo, con qué garantías en cumplimiento del capítulo V del RGPD.

c) Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga: la información recogida en el artículo 30.2 del RGPD incluidas las transferencias de datos personales a un tercer país u organización internacional (en su caso), junto con la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.

d) Si fuera necesario por la propia evolución de las necesidades de actualización de los sistemas de información utilizados por el Encargado del Tratamiento para dar el servicio del Bono, se comunicará cualquier cambio que se produzca, a lo largo del ciclo de vida de los datos, en los apartados anteriores y no se ejecutará dicho cambio hasta el visto bueno del Responsable del Tratamiento.

e) Si un encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones de interés público.

f) Solo podrán tener acceso a los datos personales aquellas personas autorizadas y únicamente para aquellos datos precisos para la ejecución del programa Bono Cultural Joven 2023 y para el fin específico que se requiera. Se deberá tener un control de las personas que tengan acceso en cada actuación del Encargado, y será evidenciable, debiendo contar con el correspondiente compromiso de confidencialidad.

g) Llevar un listado de personas autorizadas en el apartado anterior para tratar los Datos Personales objeto del tratamiento y garantizar que las mismas se comprometen a respetar la confidencialidad, y a cumplir con las medidas de seguridad correspondientes, de las que les debe informar convenientemente. Igualmente mantener a disposición del Responsable del Tratamiento dicha documentación acreditativa. Dicha documentación acreditativa no comportará en ningún caso una comunicación de datos personales de las personas autorizadas.

cve: BOE-A-2023-19756
Verificable en https://www.boe.es

h) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del Responsable del Tratamiento, en los supuestos legalmente admitidos.

i) Llevar, por escrito, un registro de todos los incidentes de seguridad de la información tanto que se deban aportar o no al CCN-CERT.

j) Para la realización del servicio, se requieren las siguientes comunicaciones internas de datos entre los Encargados del Tratamiento del Ministerio de Cultura y Deporte:

– La Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM), a través de la plataforma tecnológica de gestión del Bono Cultural Joven, contiene los datos personales correspondientes a los solicitantes de las ayudas y adhesión de las entidades al citado programa (personas interesados y representantes legales).

– TRAGSATEC obtiene, a través de la plataforma tecnológica de la FNMT-RCM, los datos personales necesarios para realizar la revisión documental de los expediente de concesión de ayudas y de adhesión de las entidades.

– La Sociedad Estatal Correos y Telégrafos, SA, S.M.E., como entidad comercializadora de medios de pago de las tarjetas prepago y de gestión de altas y bajas de TPVs de las entidades adheridas, recibe de forma segura a través de la plataforma de la FNMT-RCM mediante APIs, los datos personales necesarios de las personas beneficiarias del Bono Cultural Joven y de las entidades adheridas al programa.

k) En caso de duda en el acceso a los datos por personal autorizado o en el flujo de estos, se consultará al responsable la manera de proceder y siempre de manera que se respete la confidencialidad y la seguridad de la información.

l) El Encargado del Tratamiento siempre colaborará tanto en el cumplimiento de las obligaciones del responsable como en su demostración.

m) En el ámbito de actuación del encargado, se atenderán las siguientes indicaciones:

– No se permitirá el uso para fines particulares de aquellos ordenadores y dispositivos destinados al tratamiento de los datos personales.

– Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal, se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador o dispositivo.

– Si, en el procedimiento de tratamiento o acceso a los datos a través de un equipo de los Encargados del Tratamiento, se realice mediante acceso remoto, se debe disponer de las medidas de seguridad adecuadas contando, al menos, de una VPN y doble factor de autenticación, 2FA, o medidas de seguridad equivalentes y que cumplan con el nivel requerido del ENS para en el nivel que corresponda.

– Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que, en caso de ataque de ciberseguridad, puedan obtenerse privilegios de acceso o modificar el sistema operativo.

– Se garantizará la existencia de contraseñas (o mecanismos equivalentes) para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá, al menos, 16 caracteres, mezcla de números y letras, y se renovarán periódicamente (al menos de forma trimestral).

– Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).

cve: BOE-A-2023-19756
Verificable en https://www.boe.es

– Se garantizará la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

– Actualización de ordenadores y dispositivos. Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.

– En los ordenadores y dispositivos donde se realice el tratamiento de los datos personales, se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.

– Para evitar accesos remotos indebidos a los datos personales, se velará para garantizar la existencia de un cortafuegos activado en aquellos sistemas en los que se realice el almacenamiento y/o tratamiento de datos personales.

– Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de cifrado para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.

– En la parte del flujo de trabajo de cada Encargado del Tratamiento y como refuerzo al apartado a), periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el equipo con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información. La copia de seguridad debe estar encriptada.

– Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará: dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia, si lo hubiera. Cuando la persona se ausente del puesto de trabajo, procederá al bloqueo de la pantalla o al cierre de la sesión.

– Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día, y serán custodiados cuando, con motivo de su tramitación, se encuentren fuera de los dispositivos o salas de archivo.

– No se desecharán documentos (papel) o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción, de forma que la información no sea recuperable.

Elementos del tratamiento.

El tratamiento de los Datos Personales comprenderá: registro (grabación), estructuración, modificación, consulta, interconexión (cruce), cotejo, supresión, destrucción (de copias temporales), conservación (en sus sistemas de información), copia de seguridad y recuperación.

Disposición de los datos al finalizar la colaboración.

a) Una vez finalice la vigencia del convenio, el encargado (y sus subencargados implícitamente) deben: devolver al responsable del tratamiento 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 los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

cve: BOE-A-2023-19756
Verificable en https://www.boe.es

No obstante, y previa notificación por escrito del Responsable del Tratamiento a la finalización del encargo, el Responsable del Tratamiento podrá requerir al encargado para que en vez de la opción a), cumpla con la b) o c) siguientes:

b) Devolver al encargado que designe por escrito el responsable del tratamiento, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

c) Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y previa petición, debe entregar el certificado al responsable del tratamiento. No obstante, el encargado puede conservar una copia, con los datos debidamente boqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Medidas de seguridad.

Los datos deben protegerse para evitar que dichos datos pierdan su razonable confidencialidad, integridad y disponibilidad y de acuerdo con la catalogación del riesgo según el anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y la evaluación de riesgos realizada. Se deben implantar, al menos, las siguientes salvaguardas:

1. Privacidad desde el diseño y por defecto.

Tipo	Descripción	Salvaguardas
Ocultación o pseudonimización (RGPD).	Los datos a comunicar se deben ofuscar.	Si aparece información del entorno de producción, se disociarán los datos identificativos.
Borrado de información.	Se deben establecer criterios concretos para eliminar los datos.	Se deben definir criterios generales de borrado, conforme a los plazos legales de conservación.
Seguridad en los requisitos, análisis y diseño de aplicaciones informáticas.	El modelo de datos debe incluir el mínimo número de datos, la exposición de los datos debe predefinirse teniendo en cuenta los requisitos de seguridad.	Análisis de PbDD. Debe existir una lista de requisitos de seguridad. Un informe debe relacionar los requisitos de seguridad con las medidas de análisis implantadas, y detectar mejoras.
Seguridad en la puesta en producción de aplicaciones informáticas.	Se debe garantizar que las aplicaciones informáticas tienen controles de seguridad adecuados.	Evaluar que la aplicación tiene control de accesos. Controlar que las aplicaciones no sean vulnerables al top 10 de OWASP.
Cancelación periódica / Expurgo.	El modelo de datos debe incluir el mínimo número de datos, la exposición de los datos debe predefinirse teniendo en cuenta los requisitos de seguridad.	Definir y aplicar criterios generales de conservación de la información. Definir procedimientos de expurgo de la información aprobados, y conocidos, por la Organización. Auditar anualmente los procedimientos de cancelación periódica y expurgo. Valorar la contratación de un proveedor certificado en procedimientos de destrucción segura de información.
Finalidades debidas y no excesivas.	Las finalidades deben ser debidas y no excesivas.	Definir finalidades específicas.
Políticas de control de accesos.	Restringir el acceso a los datos bajo el principio de necesidad de conocimiento.	Implementar controles de acceso a la información.
Técnicas de ofuscación o disociación.	Los datos deben ser ininteligibles mediante cifrado, u optar por eliminar la vinculación entre conjuntos de datos independientes.	Se debe eliminar la vinculación entre diferentes conjuntos de datos, manteniéndolos independientes.

cve: BOE-A-2023-19756
Verificable en https://www.boe.es

Tipo	Descripción	Salvaguardas
Técnicas de agregación.	Agrupar la información relativa a varios sujetos usando técnicas de generalización y supresión.	Se debe agrupar la información relativa a varios sujetos, no utilizando los datos del sujeto específico.
Tratar sólo las muestras de sujetos relevantes para la finalidad.	Elegir sólo la muestra de sujetos relevante y los atributos necesarios para el tratamiento; u optar por excluir previamente los sujetos y atributos irrelevantes para el tratamiento realizado.	Revisar los datos necesarios para el tratamiento y almacenamiento.
Técnicas de eliminación de los datos.	Eliminar parcialmente los datos cuando dejen de ser necesarios o suprimirlos por completo cuando dejen de ser relevantes, asegurándose de que no sean recuperables.	Si aparece información del entorno de producción, se deben disociar los datos identificativos.
Técnicas de sumarización de los datos.	Generalizar los valores de los atributos utilizando intervalos o rangos de valores, en lugar de un valor concreto.	Se deben utilizar rangos de valores simples.
Técnicas de agrupación de los datos.	Agregar la información de un grupo de registros en categorías, en lugar de utilizar información detallada de cada sujeto.	Aplicar una agregación en el tiempo.
Técnicas de perturbación de los datos.	Perturbar: utilizar valores aproximados o modificar el dato real mediante el empleo de algún tipo de ruido aleatorio en lugar de trabajar con el valor exacto del dato.	Aplicar técnicas de ofuscación simples.
Separación de los datos.	Recoger y almacenar los datos en distintas BBDD o apps independientes lógica y físicamente, adoptando medidas adicionales de desvinculación como el borrado programado de tablas de indexación.	Compartimentar el acceso a los datos.
Distribuir los datos.	Diseminar la recogida y tratamiento de los subconjuntos de datos correspondientes a diferentes tratamientos sobre unidades de tramitación y gestión que sean físicamente independientes y utilicen sistemas y apps diferentes.	La recogida de los datos se debe realizar por departamentos diferentes de quienes van a realizar el tratamiento.
Recogida del consentimiento del titular de los datos (apps móvil).	Recoger el consentimiento de los titulares de forma inequívoca, mediante manifestación o clara acción afirmativa. Debe ser revocable.	Buscar bases de legitimación alternativas al consentimiento.
Alertar al interesado (apps móvil).	Se debe informar al interesado del momento en que se está realizando una recogida de datos, aun cuando ya haya sido informado de forma genérica de la base legal que justifica el tratamiento, o haya prestado consentimiento.	El consentimiento debe ser informado.
Elección por el interesado de la forma de tratamiento (apps móvil).	Proporcionar la funcionalidad granulada de apps y servicios, sin supeditarla al consentimiento del tratamiento de datos innecesarios para su ejecución.	El consentimiento debe ser específico.
Mecanismos de actualización de los datos (apps móvil).	Implementar mecanismos que faciliten a los usuarios o incluso les permita revisar, actualizar y rectificar directamente los datos para los que se haya facilitado un tratamiento concreto.	La Organización debe contar con procedimientos para gestionar las solicitudes de actualización de información en las tarjetas virtuales.
Mecanismos de supresión de los datos.	Proporcionar mecanismos para que los usuarios puedan suprimir o solicitar el borrado de los datos personales que hayan facilitado a un responsable.	Contar con Procedimientos de Gestión de Derechos.

cve: BOE-A-2023-19756
Verificable en https://www.boe.es

Tipo	Descripción	Salvaguardas
Política de Protección de Datos.	Especificar una política de protección de datos que refleje las cláusulas de privacidad comunicadas a los interesados. Desarrollar procesos de formación y concienciación.	Contar con Procedimientos sobre gestión de obligaciones del RGPD.
Medidas técnicas y organizativas que ejecuten la Política.	Dar soporte a la política definida mediante el establecimiento y revisión de mecanismos y procedimientos de cumplimiento efectivo e implantación de medidas técnicas y organizativas necesarias.	Realizar análisis de riesgos en seguridad de la información.
Garantizar el cumplimiento de la Política de Privacidad.	Asegurar el cumplimiento, eficacia y eficiencia de la política de privacidad y de los procedimientos, medidas y controles implantados.	Debe existir un Responsable de Seguridad, o rol similar, en cada entidad y un delegado de protección de datos.
Auditoría.	Revisar de forma sistemática, independiente y documentada el grado de cumplimiento de la política de protección de datos.	Realizar una autoevaluación periódicamente y una auditoría interna en caso de evaluación negativa. El responsable dispondrá de todas las facilidades en caso de proceder a una auditoría con tanto siempre con una persona de suficiente rango en al entidad que sirva de contacto y para el correcto desarrollo de la misma.
Registro de decisiones y cambios.	Documentar todas y cada una de las decisiones tomadas en el tiempo, aun cuando hayan resultado contradictorias, identificando quién las tomó, cuándo y justificación para hacerlo.	Los documentos deben contener registros de cambios.
Notificar eventos de seguridad.	Documentar los resultados de las auditorías realizadas y cualquier incidente que se produzca en operaciones de tratamiento de datos, y ponerlo a disposición de la autoridad.	Informar al Responsable a la mayor brevedad posible de los incidentes de seguridad, antes de 24 horas desde su descubrimiento.
Informar a los interesados.	Suministrar a los interesados la información exigida por el RGPD de forma concisa, transparente, inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo.	Las cláusulas de información deben ser actualizadas al RGPD.
Informar a los interesados.	Informar sobre el tratamiento a los interesados, cuando los datos no se recaben directamente de ellos, en el momento en que sean obtenidos y a más tardar en el plazo de un mes.	Informar a los interesados cuyos datos no se recabaron directamente de ellos.

2. Seguridad informática.

Tipo	Descripción	Salvaguardas
Protección de las instalaciones e infraestructuras (ENS).	RD 311/2022, anexo II. Las instalaciones e infraestructuras deben tener medidas de seguridad física.	Implementar controles de acceso físico a edificios y sistemas contra incendios.
Protección frente a código dañino (ENS).	RD 311/2022, anexo II., op.exp. Deben existir sistemas antimalware.	Instalar software antimalware en equipos personales.
Aislamiento de datos en entornos productivos (ENS).	Los datos fuera del entorno de producción no deben ser reales, o bien estar convenientemente protegidos.	El entorno de producción debe estar aislado del resto de entornos.
Cifrado de información almacenada (ENS).	RGPD. Debe guardarse cifrada la información almacenada en bases de dato o ficheros informáticos.	Se deben cifrar los datos más sensibles (domicilio, etc.).

cve: BOE-A-2023-19756
Verificable en https://www.boe.es

Tipo	Descripción	Salvaguardas
Caracterización del puesto de trabajo (ENS).	RD 311/2022, anexo II. mp.per.1. El puesto de trabajo debe estar definido con requisitos de seguridad establecidos.	Se deben clasificar los puestos de trabajo en función del volumen y la sensibilidad de la información a la que pueden acceder.
Configuración de seguridad (ENS).	RD 311/2022, anexo II. (op.exp.2 ENS). Los sistemas informáticos en producción deben estar configurados para soportar ataques o malas manipulaciones.	Se deben analizar las vulnerabilidades de los equipos en producción. Se deben deshabilitar los servicios no usados.
Protección telecomunicaciones.	Los datos se deben transmitir cifrados.	Se deben cifrar las comunicaciones.
Protección de ficheros temporales.	Los ficheros temporales se deben proteger igual que los datos maestros.	Se debe elaborar un inventario de ficheros temporales.
Medidas de protección de la documentación.	Medidas de protección de la documentación.	La información en papel se debe guardar en espacios con control de acceso.
Identificación y autenticación.	Se debe controlar que un usuario es quien dice ser (RD 311/2022, anexo II).	Se debe utilizar Usuario y Contraseña y doble factor de autenticación (2FA).

3. Sobre el concepto de proceso.

Tipo	Descripción	Salvaguardas
Gestión y distribución de soportes (ENS).	(mp.si.2 ENS, criptografía para dispositivos removibles). Los soportes se deben proteger en su almacenamiento y distribución.	Inventariar los soportes y enviar cifrados.
Procedimiento de autorización (ENS).	RD 311/2022, anexo II. Org.4. Control de que un usuario sólo accede a los servicios que tenga autorizados.	Debe existir un procedimiento formal de autorización.
Segregación de funciones y tareas (ENS).	RD 311/2022, anexo II: (op.acc.3 ENS), las funciones están separadas.	Los trabajadores que acceden al entorno de producción no deben ser los mismos que acceden al entorno de desarrollo.
Notificación violaciones seguridad (ENS).	(ART.33 y 34 RGPD) Se deben gestionar, registrar y notificar las incidencias/violaciones de seguridad.	Se deben notificar las violaciones graves de seguridad a la autoridad de control, al CCN y a los titulares de los datos lo más pronto posible y siempre antes de las 72 horas.
Formación.	Se debe impartir formación.	Sin requisitos especiales.
Asesoramiento experto.	Se debe contar con asesoramiento experto.	Se debe implantar una web con contenidos de preguntas frecuentes. El DPD del encargado debe hacer un asesoramiento personalizado..
Cláusulas informativas.	Se debe contar con cláusulas informativas.	Deben existir cláusulas publicadas con el nombre del tratamiento, su responsable y el resto de información que exige el RGPD.
Legitimación de transferencias internacionales y cesiones de datos.	Se deben legitimar las transferencias internacionales y comunicaciones de datos.	Las transferencias internacionales se deben declarar en los datos de registro del tratamiento.
Pruebas con datos reales.	Los datos fuera del entorno de producción no deben ser reales o bien deben estar convenientemente protegidos.	Se debe disociar el nombre, apellidos y DNI antes de cargar datos de prueba a partir de datos de producción.

cve: BOE-A-2023-19756
Verificable en https://www.boe.es

Tipo	Descripción	Salvaguardas
Actualización periódica de la información.	Se debe garantizar la actualización periódica de la información.	Sin requisitos especiales.
Autorización de subcontrataciones.	Autorización de subcontrataciones.	(Si hay subcontrataciones) El encargado de tratamiento debe solicitar por escrito al responsable del tratamiento la autorización de las subcontrataciones.

4. Rendición de Cuentas (ayuda al Responsable del Tratamiento).

Tipo	Descripción	Salvaguardas
Auditorias de cumplimiento.	(RD 311/2022 y ART.96) Se deben realizar auditorías de seguridad.	Realizar una auditoría anual de cumplimiento RGPD. Puede hacerla cada encargado internamente sin perjuicio de que el Responsable encargue una a su vez.
Trazabilidad / Registro de Accesos (ENS).	Registrar y analizar los accesos al sistema de información y a las bases de datos.	Registrar los accesos a los datos de lectura y actualización.
Revisión de la privacidad desde el diseño y por defecto.	Comprobar periódicamente que las medidas de privacidad están operativas.	Realizar una revisión en la puesta en marcha del tratamiento.
Cumplimiento deber de secreto.	Se debe cumplir el deber de secreto.	Cada trabajador que accede a los datos debe firmar un contrato de confidencialidad.
Contratos de encargo y cumplimiento de las obligaciones por el prestador.	Los contratos de encargo deben cumplir con los requisitos legales, y debe garantizarse el cumplimiento de las obligaciones por el prestador.	Se debe solicitar un compromiso escrito (declaración responsable) a los encargados de tratamiento de que cumplen con las medidas de seguridad impuestas por el responsable del tratamiento.

La entidad colaboradora no podrá no implementar o suprimir estas salvaguardas mediante el empleo de un análisis de riesgo o evaluación de impacto propia salvo aprobación expresa de la Subsecretaría de Cultura y Deporte.

A estos efectos, el personal del encargado del tratamiento debe seguir las medidas de seguridad establecidas, no pudiendo efectuar tratamientos distintos de los definidos por la Subsecretaría de Cultura y Deporte.»

Segunda. *Información a representantes, trabajadores y personas de contacto.*

Los datos personales de los representantes de las Partes, así como de sus trabajadores y resto de personas de contacto que puedan intervenir en la relación jurídica formalizada serán tratados, respectivamente, por las entidades que se identifican en el encabezamiento, que actuarán, de forma independiente, como responsables del tratamiento de los mismos. Dichos datos serán tratados para dar cumplimiento a los derechos y obligaciones contenidas en esta adenda, sin que se tomen decisiones automatizadas que puedan afectar a los interesados. En consecuencia, la base jurídica del tratamiento es dar cumplimiento a la mencionada relación de colaboración en la gestión del programa, siendo dicho fin estrictamente necesario para ejecutar la presente adenda.

Los datos se mantendrán mientras esté en vigor la relación de colaboración que aquí se estipula, siendo tratados únicamente por las Partes y aquellos terceros a los que aquéllas estén legal o contractualmente obligados a comunicarlos (como es el caso de terceros prestadores de servicios a los que se haya encomendado algún servicio vinculado con la gestión o ejecución del Convenio).

Los interesados de las Partes podrán ejercer, en los términos establecidos por la legislación vigente, los derechos de acceso, rectificación y supresión de datos, así como solicitar que se limite el tratamiento de sus datos personales, oponerse al mismo, o solicitar la portabilidad de sus datos dirigiendo una comunicación por escrito a cada una de las Partes, a través de las direcciones especificadas en el encabezamiento o a través de la siguiente

cve: BOE-A-2023-19756
Verificable en https://www.boe.es

dirección de correo electrónico: derechos.protecciondatos.correos@correos.com o en la sede electrónica del Ministerio de Cultura y Deporte, según corresponda.

Asimismo, podrán ponerse en contacto con los respectivos delegados de protección de datos en la dirección dpdgrupocorreos@correos.com o dpd@cultura.gob.es según corresponda, o presentar una reclamación ante la Agencia Española de Protección de Datos u otra autoridad competente.

Las Partes se comprometen expresamente a informar a sus trabajadores y resto de personas de contacto de los términos de la presente cláusula, manteniendo indemne a la contraparte de los daños que pueda conllevar la falta de cumplimiento de esta obligación.

Tercera. *Acuerdo íntegro.*

La presente adenda comprende la totalidad de los pactos, acuerdos y compromisos asumidos por las partes en relación con la modificación del Convenio de Colaboración, el cual permanecerá en vigor en su totalidad en todo lo no modificado por esta adenda.

Y, en prueba de conformidad de cuanto antecede, y para la debida constancia de todo lo convenido, las Partes firman la presente Adenda electrónicamente, tomándose como fecha de formalización del presente documento la fecha del último firmante.–La Subsecretaria del Ministerio de Cultura y Deporte, María Pérez Sánchez-Laulhé.–La Directora de Filatelia, Estudios y Futuro de la Sociedad Estatal Correos y Telégrafos, Leire Diez de Castro.–La Directora de Relaciones Institucionales de la Sociedad Estatal Correos y Telégrafos, Nuria Lera Hervás.

cve: BOE-A-2023-19756
Verificable en https://www.boe.es