Normativa, información y consentimiento relativos a protección de datos de trabajadores y colaboradores de BFIS

NOMBRE Y APELLIDOS:	

RESUMEN DE ESTE DOCUMENTO

Con el objetivo de dar cumplimiento a la normativa de protección de datos, Fundación Privada Benjamin Franklin – Benjamin Franklin International School (en adelante BFIS) estipula en este documento:

(A) Información relativa al tratamiento de los datos del trabajador/colaborador
(B) El deber de confidencialidad y secreto
(C) Medidas de seguridad obligatorias para todos los trabajadores/colaboradores y régimen de autorizaciones.
(D) Consentimiento del trabajador/colaborador en relación al tratamiento de sus datos personales para determinadas finalidades accesorias a la relación laboral, de colaboración o prestación de servicios.

1. El **responsable del tratamiento** de los datos del trabajador/colaborador es BFIS.

2. La **finalidad del tratamiento de los datos** es gestionar la relación laboral, de colaboración o prestación de servicios con el trabajador/colaborador, y otras finalidades relacionadas según se indica en la información detallada (apartado A).

3. La **base legal del tratamiento** de los datos es la ejecución de un contrato y el cumplimiento de obligaciones legales de BFIS, así como el consentimiento del trabajador/colaborador para las finalidades especificadas en el apartado D.

4. Los **destinatarios de la información** son las autoridades competentes, así como otros destinatarios especificados en este documento incluido lo establecido en la información detallada (apartado A).

5. Posibilidad del trabajador de ejercer los **derechos** de acceso, rectificación, y supresión, y demás derechos de protección de datos, según se puede consultar en este documento.

6. **Confidencialidad y deber de secreto** por parte del trabajador/colaborador en relación a cualquier información a la que tenga acceso al desempeñar sus funciones en BFIS, según se detalla en el apartado B "Confidencialidad y deber de secreto", obligación que subsiste una vez extinguida la relación con BFIS.

7. El trabajador/colaborador cumplirá las **medidas de seguridad** establecidas en BFIS, incluyendo el **régimen de autorización correspondiente** y **medidas técnicas y organizativas** para garantizar la seguridad de los datos y de los recursos, incluyendo su protección contra el tratamiento no autorizado o ilícito, su pérdida, destrucción o daño, según se detalla en el apartado C "Medidas de seguridad y régimen de autorización".

A - INFORMACIÓN SOBRE EL TRATAMIENTO DE LOS DATOS RELATIVOS AL TRABAJADOR / COLABORADOR

En este apartado BFIS le facilita de forma detallada la información adicional relativa al tratamiento de sus datos personales como trabajador/colaborador.

1. Responsable del tratamiento de los datos: FUNDACIÓN PRIVADA BENAJMIN FRANKLIN, CIF G58203522. Domicilio: MARTORELL I PEÑA, 9, 08017, BARCELONA.

2. Finalidad del tratamiento de los datos. Los datos se tratan para las siguientes finalidades:

- **Gestión de la relación con el trabajador/colaborador** (ya sea laboral, de prestación de servicios o colaboración, contrato de prácticas, becarios, etc) y en su caso del expediente del trabajador
- Realizar todos aquellos **trámites administrativos, fiscales y contables** necesarios para cumplir con los compromisos contractuales, obligaciones en materia de normativa laboral, Seguridad Social, prevención de riesgos laborales, fiscal y contable.
- **Gestión de pago** de nóminas mediante entidad financiera.
- En su caso, realizar **actuaciones formativas** tanto de formación bonificada como no bonificada.

- **Registro diario de jornada laboral (control horario)** a través del sistema de control que se habilite
- Utilización de sistemas de **videovigilancia** para: **seguridad**, tanto de los clientes como trabajadores/colaboradores, **control de accesos** a las instalaciones, así como realizar un **control del cumplimiento de las obligaciones del trabajador/colaborador**. Las zonas vigiladas estarán convenientemente señalizadas
- Respecto a los recursos informáticos, correo electrónico profesional o acceso a internet que proporcione BFIS, se monitorizaran para control de las obligaciones del trabajador/colaborador así como verificar su buen uso.
- En relación a las finalidades de control del cumplimiento de las obligaciones del trabajador/trabajador, informamos que la información obtenida mediante los sistemas de videovigilancia podrá utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo o de la relación de prestación de servicios.
- Gestión de todos aquellos beneficios sociales o sistemas de retribución flexible o ventajas exclusivas por su condición de empleado (cheque restaurante, cheque guardería, seguros de salud, etc).
- En el caso del certificado negativos penales, la finalidad es la de cumplir con los requisitos legales.

Los datos también serán tratados para aquellas otras finalidades para las que el trabajador/colaborador haya consentido expresamente.

3. Plazo de conservación de los datos del trabajador por parte de BFIS. Los datos personales serán conservados mientras dure la relación con BFIS. Al finalizar la misma, los datos personales tratados para cada una de las finalidades indicadas se mantendrán durante los plazos legalmente previstos o durante el plazo que una autoridad pública, un juez o tribunal los pueda requerir atendiendo al plazo de prescripción de acciones administrativas y/o judiciales. Los datos tratados en base al **consentimiento** del interesado se mantendrán en tanto el interesado no solicite su supresión o revoque el consentimiento otorgado y en cualquier caso hasta que expiren los plazos legales aludidos anteriormente, si hubiera obligación legal de mantenimiento.

Las **imágenes** captadas por los sistemas de videovigilancia se conservarán durante el plazo máximo de un mes desde su captación, pudiendo conservarse durante el plazo necesario en caso de captarse cualquier incidente relevante.

4. Legitimación para el tratamiento de los datos personales y manifestación de consentimiento. La base legal para el tratamiento de los datos es la ejecución del contrato laboral, de colaboración o prestación de servicios. Los datos también se tratan en cumplimiento de las obligaciones legales en materia laboral, prevención de riesgos laborales, seguridad social, y tributaria. Para otros tratamientos accesorios y opcionales, el consentimiento será la base jurídica para el tratamiento, mediante manifestación de la voluntad del trabajador/colaborador:

5. Destinatarios de la información. Los datos serán comunicados a las entidades y organismos que se detallan a continuación:

- A las entidades bancarias que corresponda, para estar al corriente de pagos.
- A la Administración tributaria.
- Organismos de la Seguridad Social, Mutua de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social.
- En su caso, a la Inspección de Trabajo.
- A las entidades que participen en la gestión de cursos de formación a los que desee asistir el trabajador con la finalidad de participar en los cursos que se organicen.
- En su caso, al Sindicato al que se encuentra afiliado para el descuento de la cuota obrera.
- En el caso de utilizar vehículos de empresa (incluyendo renting o alquiler), a las autoridades que en su caso lo requieran, y en todo caso, para la identificación del conductor en caso de infracción de tráfico. También podrán ser comunicados, en su caso, a la compañía de alquiler/renting de vehículos.
- Agencias de viaje, compañías de transporte, establecimientos, seguros de viaje, etc. en el marco de viajes relacionados con BFIS, en caso de gestionar sus billetes, alojamiento y reservas necesarias.
- Entidades contratantes siempre que sea imprescindible en cumplimiento de normativa de contratación vigente.
- Entidades que conceden subvenciones a BFIS, dentro de la documentación que se deba proporcionar dentro de las condiciones de la subvención.
- Entidades organizadoras de cursos. En estos pueden estar situados fuera de la Unión Europea.

6. Derechos en relación con el tratamiento de datos. El trabajador/colaborador tiene derecho a:

- acceder a sus datos personales.
- solicitar la rectificación de los datos que sean inexactos o, en su caso, solicitar la supresión, cuando entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos o cuando el trabajador/colaborador retire el consentimiento otorgado.
- en determinados supuestos el trabajador/colaborador podrá solicitar la limitación del tratamiento de sus datos, en cuyo caso solo se conservarán de acuerdo con la normativa vigente.

- en ciertos supuestos el trabajador/colaborador podrá ejercitar su derecho a la portabilidad de los datos, que serán entregados en un formato estructurado, de uso común o lectura mecánica.
- el trabajador/colaborador tendrá derecho a revocar en cualquier momento el consentimiento para cualquiera de los tratamientos para los que lo ha otorgado.

El trabajador/colaborador tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos en el supuesto de que considere que no se ha atendido convenientemente el ejercicio de sus derechos.

En el caso de producirse alguna modificación de sus datos, el trabajador/colaborador debe comunicarlo por escrito a BFIS con la finalidad de mantener los datos actualizados.

7. Transferencias internacionales de datos. BFIS no tiene previsto realizar transferencias internacionales de datos, en caso de ser necesarias a efectos de almacenamiento, solo se realizarán a entidades bajo la habilitación del acuerdo EEUU-Unión Europea Privacy Shield (más información: https://www.privacyshield.gov/welcome), a entidades que hayan demostrado que cumplen con el nivel de protección y garantías de acuerdo con los parámetros y exigencias previstas en la normativa vigente en materia de protección de datos, como el Reglamento Europeo, o cuando exista un habilitación legal para realizar la transferencia internacional.

8. Origen y procedencia de los datos. En caso de estudiantes en prácticas, sus datos personales necesarios han sido proporcionados por la universidad o centro de formación que ha suscrito con BFIS convenio de colaboración o prácticas. En caso de personal externo, sus datos personales necesarios son proporcionados por su empresa..

B - CONFIDENCIALIDAD Y DEBER DE SECRETO

Todo el personal de BFIS, en el marco de la relación laboral o de colaboración o prestación de servicios que le une con BFIS se compromete a: /

1. No revelar a ninguna persona ajena a BFIS sin el consentimiento de BFIS, la información referente a la que haya tenido acceso durante el desempeño de sus funciones en BFIS, excepto en el caso de que ello sea necesario para dar debido cumplimiento a sus obligaciones u obligaciones de BFIS impuestas por leyes o normas que resulten de aplicación, o sea requerido para ello por mandato de la autoridad competente con arreglo a Derecho.

2. Utilizar la información que alude el apartado anterior únicamente en la forma que exija el desempeño de sus funciones en BFIS y no disponer de ella de ninguna otra forma o con otra finalidad.

3. No utilizar de ninguna forma cualquier otra información que hubiese podido obtener prevaliéndose de su condición de empleado o colaborador y que no fuera necesaria para el desempeño de sus funciones en BFIS.

4. Cumplir, en el desarrollo de sus funciones en la entidad BFIS, la normativa vigente, relativa a la protección de datos de carácter personal y, en particular, el Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos) y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales**.**

5. Cumplir los compromisos anteriores incluso después de extinguida, por cualquier causa, la relación laboral o de prestación de servicios que le une con BFIS..

En caso de ser Delegado Sindical o miembro del Comité de Empresa, le informamos que el Estatuto de los Trabajadores, establece un deber de sigilo con respecto a aquella información que, en legítimo y objetivo interés de la entidad o del centro de trabajo, les haya sido expresamente comunicada con carácter reservado. En todo caso, tal y como establece el Estatuto de los Trabajadores, ningún tipo de documento entregado por la empresa al Comité podrá ser utilizado fuera del estricto ámbito de la misma ni para fines distintos de los que motivaron su entrega. El deber de secreto subsistirá incluso tras expirado su mandato e independientemente del lugar en que se encuentre.

C - MEDIDAS DE SEGURIDAD Y RÉGIMEN DE AUTORIZACIÓN

Las siguientes medidas de seguridad son de obligado cumplimiento para todo el personal y colaboradores de BFIS en relación con el Reglamento (UE) 2016/679 (Reglamento general de protección de datos)

1. Régimen de autorización e instrucciones.

BFIS ha designado a JOSEP PABLO (contacto josepp@bfischool.org) como **RESPONSABLE DE SEGURIDAD**. En relación al mismo, el trabajador/colaborador deberá:

- Seguir las instrucciones del RESPONSABLE DE SEGURIDAD en relación al uso de los sistemas de información, medidas de seguridad de la información y tratamiento de los datos.

- Solicitar autorización cuando necesite utilizar los recursos de BFIS tales como equipos informáticos, dispositivos móviles o portátiles, sistemas de información, sistemas de videovigilancia, correo corporativo, conexión a Internet, etc. distintos a los que le hayan sido proporcionados.
- Solicitar autorización para cualquier operación conforme a lo establecido en este documento, inclusive en lo relativo a la reconfiguración de los sistemas o dispositivos, la instalación de aplicaciones o APPS, la instalación de cuentas corporativas o de e-mail, la utilización de unidades de almacenamiento, la salida de documentos y dispositivos fuera de BFIS, la utilización de servicios de almacenamiento en Internet y la utilización de dispositivos propiedad del trabajador/colaborador. .

Asimismo, BFIS ha designado a MIGUEL MARTINEZ HERNANDO (contacto: dpo@bfischool.org) como **DELEGADO DE PROTECCIÓN DE DATOS**. En relación al mismo, el trabajador/colaborador deberá:

- Atender a sus requerimientos de información, facilitándole a la mayor brevedad posible cuanta información hubiera solicitado, relativa al tratamiento de los datos personales y el uso de los sistemas.
- Informarle con carácter previo sobre nuevos tratamientos que involucren datos personales que se vayan a realizar, y que afecten a cualquier información concerniente a personas físicas identificadas o identificables.
- Informarle con carácter previo sobre cambios organizativos o técnicos que puedan tener alguna consecuencia o suponer un riesgo para las personas cuyos datos sean objeto de tratamiento.
- Informarle sobre nuevos prestadores de servicios que vayan a acceder a los datos, o que puedan almacenarlos o que tengan un acceso físico al lugar donde están los datos.
- Informarle sobre brechas e incidentes de seguridad con los datos tan pronto como se tenga constancia de los mismos, según lo establecido más adelante.
- Informarle sobre la recepción de solicitudes de ejercicio de derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento, según lo establecido más adelante.
- Informarle sobre la transferencia internacional de datos fuera del Espacio Económico Europeo que prevea realizar.

2. Prohibición del uso particular de los recursos de BFIS. Todos los recursos de BFIS incluyendo conexión a Internet, ordenadores y dispositivos móviles o portátiles, son para fines estrictamente de BFIS y por tanto no se utilizarán para fines particulares.

BFIS informa de que podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador/colaborador de sus obligaciones, guardando en su adopción y aplicación la consideración debida a su dignidad humana.

Entre los sistemas de control previstos se encuentra el registro y revisión de la navegación, alertas automáticas sobre el envío de mensajes con adjuntos y la revisión de los correos electrónicos sospechosos, así como el acceso a los mismos durante la ausencia del usuario en caso que sea necesario.

3. Incidentes con los datos personales. Todo incidente de seguridad o brecha en los datos personales que pueda afectar documentos, tanto en soporte papel como en archivo informático, dispositivos o recursos informáticos deberá comunicarse de forma inmediata, al RESPONSABLE DE SEGURIDAD o DELEGADO DE PROTECCIÓN DE DATOS.

4. Ejercicio de derechos. Cualquier solicitud de ejercicio de derechos por parte de un interesado en relación con el tratamiento de sus datos será trasladada inmediatamente al RESPONSABLE DE SEGURIDAD o DELEGADO DE PROTECCIÓN DE DATOS.

5. Manejo de documentos de BFIS. En relación a cualquier documento o información en soporte papel, perteneciente a BFIS, al que tenga acceso el trabajador/colaborador:

- El trabajador/colaborador custodiará los documentos para impedir su visualización, acceso o manipulación por otras personas y/o personas no autorizadas.
- Los documentos se guardarán bajo llave.
- La generación de copias requerirá autorización
- El desecho de los documentos requerirá su destrucción o triturado de forma que se impida recuperar la información a posteriori.

En relación con documentos/archivos informáticos que contengan datos personales, es responsabilidad del trabajador/colaborador que los ha creado y de aquellos que tengan permisos de edición, evitar un acceso indebido a los mismos o revelación indebida ubicándolos en unidades de acceso restringido, configurando de forma restrictiva los permisos de acceso/visionado, limitando la posibilidad de compartir el/los archivos/documentos y deshabilitando la posibilidad de descarga, impresión y copia.

6. Contraseñas. En relación a las contraseñas que en su caso se proporcionen al trabajador/colaborador, se renovarán al menos una vez al año, se evitarán contraseñas cortas o fáciles de adivinar, y se mantendrán completamente confidenciales, en ningún caso se comunicarán a terceras personas o se anotarán en lugares visibles.

7. Reconfiguración y/o instalación de aplicaciones o APPS. En relación a los ordenadores y dispositivos fijos o portátiles, pertenecientes a BFIS, la reconfiguración de los mismos, la instalación de aplicaciones o APPS, o la instalación de cuentas corporativas o cuentas de e-mail requerirá autorización.

8. Unidades de almacenamiento (memorias USBs, discos, tarjetas de memoria, etc) únicamente se podrán utilizar con autorización.

9. Bloqueo de dispositivos portátiles / móviles. Deberá activarse el sistema de bloqueo (ej código) o protección disponible en el dispositivo, de forma que se impida su utilización por personas no autorizadas.

10. Salida de documentos y dispositivos. La salida de documentos y dispositivos informáticos fuera de los locales de BFIS precisa de autorización./

11. Ficheros temporales. Todos los ficheros temporales deberán ser borrados, una vez haya finalizado la finalidad para la que fueron creados.

12. Servicios de almacenamiento en Internet. Queda prohibido el uso de aplicaciones en la nube para compartir documentos o trabajar fuera del lugar de trabajo, que no estén previamente autorizadas por BFIS. Esto afecta al uso de aplicaciones tales como: Dropbox, Wetransfer, Office 365, Google Drive o Gmail. A la hora de autorizarlos, BFIS únicamente aceptará aquellos servicios prestados por entidades adheridas al acuerdo EEUU-Unión Europea Privacy Shield, a entidades que hayan suscrito cláusulas contractuales tipo, o a entidades que presten su servicio desde países con una legislación de protección de datos equiparable a la europea a juicio de las autoridades de protección de datos.

13. Utilización de ordenadores o dispositivos particulares para asuntos de BFIS. La utilización de ordenadores o dispositivos particulares (es decir, que no pertenecen a BFIS) no se autoriza salvo autorización expresa. Cuando se autorice, al utilizar estos dispositivos, se tendrá en cuenta lo siguiente:

- Cuando el mismo ordenador o dispositivo se utilice por personas diferentes, deberán disponer de varios perfiles o usuarios distintos, debiendo mantenerse separados los usos para asuntos de BFIS de otros usos del dispositivo./
- Se dispondrá 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 de BFIS. 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 para el acceso a los datos personales de BFIS. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras, y se cambiará todos los años.
- Cada persona con acceso a los datos BFIS dispondrá de un usuario y contraseña específicos.
- Se activará un sistema de bloqueo cuando el ordenador o dispositivo esté inactivo, siendo necesario reintroducir la contraseña o bien un código de desbloqueo o sistema equivalente disponible en el dispositivo.
- Se debe garantizar 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.
- Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.
- Se seguirán las recomendaciones del fabricante del sistema operativo en relación a la utilización de sistemas antivirus.
- Si activará el cortafuegos del ordenador o dispositivo si éste está disponible
- Cuando se precise realizar la extracción de datos personales fuera del ordenador o dispositivo, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
- Periódicamente se realizará una copia de seguridad en un dispositivo distinto del que se utiliza para el trabajo habitual. 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.

14. Todos los compromisos anteriores deben mantenerse, incluso después de extinguida la relación con BFIS.

15. Las normas y protocolos establecidos en el presente documento forman parte de las obligaciones laborales del trabajador, por lo que su incumplimiento podrá acarrear una sanción disciplinaria, incluyendo el despido, sin perjuicio de que dicha conducta pueda ser constitutiva de un delito (delito de revelación de secretos, delito de daños informáticos, etc), cuya responsabilidad se dirimirá siguiendo los cauces judiciales correspondientes.

Asimismo, el trabajador/colaborador podrá ser considerado responsable frente a BFIS y frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de las normas establecidas en este documento por lo que BFIS se reserva el derecho de exigir el resarcimiento de las indemnizaciones, sanciones o reclamaciones que se viera obligada a satisfacer como consecuencia de dicho incumplimiento.

D - MANIFESTACIÓN DE CONSENTIMIENTO DEL TRABAJADOR/COLABORADOR PARA DETERMINADAS FINALIDADES ACCESORIAS A LA RELACIÓN LABORAL, DE COLABORACIÓN O PRESTACIÓN DE SERVICIOS.

El trabajador/colaborador manifiesta su consentimiento, mediante la marcación de las casillas correspondiente, para los siguientes usos de sus datos:

SI	NO	
☐	☐	Para el tratamiento de la imagen, realización de fotografías y su utilización y publicación en el marco de su relación con BFIS y posteriormente, pudiendo ser utilizadas en el directorio o página web de la entidad, redes sociales, publicaciones, revistas del sector, con la finalidad de promocionarla. El trabajador/colaborador comprende que muchas redes sociales están ubicadas fuera del Espacio Económico Europeo, por lo que la publicación de su imagen puede constituir una transferencia internacional de datos y en cualquier caso, una cesión de datos.
☐	☐	Realización de felicitaciones, en el ámbito de la organización, de eventos como el cumpleaños, la maternidad o paternidad, o la jubilación, con la consiguiente revelación de información personal (por ejemplo la fecha de cumpleaños).
☐	☐	A la utilización del número de teléfono móvil particular a efectos de contactarle para asuntos relativos a BFIS incluyendo la transferencia de datos relacionada con el uso de APPS de terceros y la revelación del número a participantes de los grupos donde se incluya el trabajador/colaborador.
☐	☐	Cesión de datos a empresas u organizaciones que organizan cursos, incluyendo aquéllas que se encuentran fuera de la Unión Europea.

Con la firma de este documento, el trabajador/colaborador declara haberlo leído y comprendido en toda su extensión. Asimismo entiende que es su responsabilidad aclarar las dudas/preguntas que pudiera tener con el Delegado de Protección de Datos y/o el Responsable de Seguridad.

FIRMA:	
NOMBRE Y APELLIDOS:	
DNI / NIE / PASAPORTE:	
FECHA	

Data protection regulations for BFIS employees and collaborators

DISCLAIMER – The English language version of this document is a translation, for orientation-purposes only, of the original in Spanish language. The Spanish version shall always prevail.

FULL NAME:	-------- please complete and sign the Spanish language version --------

SUMMARY

In compliance with data protection regulations, Fundación Privada Benjamin Franklin – Benjamin Franklin International School (hereinafter referred as BFIS) has drafted this document that includes:

1. BFIS is the Data Controller.

2. Purposes to process data: manage the employment/collaboration relationship, as well as other purposes as indicated below.

3. Lawful basis: processing necessary to execute a contract (employment/collaborator), to comply with the law, and consent.

4. Recipients of personal data may be public administration, supervisory authorities and others as indicated down below.

5. Employees / Collaborators have the right to be informed, right to access, right to rectification, right to erasure, and other rights as indicated in this document and in data protection regulations.

6. Employee/collaborator confidentiality and duty of secrecy with regards to information of any kind to which he/she has access when performing his/her duties at BFIS.

7. The employee/collaborator must adhere to the security measures put in place by BFIS. This includes being subject to authorizations and arranging the technical and organizational measures as indicated in this document.

A - INFORMATION ON PROCESSING OF EMPLOYEE'S / COLLABORATOR'S PERSONAL DATA

Under letter A, BFIS is providing you with additional information regarding the processing of your personal data as en employee/collaborator.

1. Data Controller: FUNDACIÓN PRIVADA BENAJMIN FRANKLIN, CIF G58203522. Domicilio: MARTORELL I PEÑA, 9, 08017, BARCELONA

2. Purpose to process your personal data:

- Manage the employment relationship and the employee's file.
- Perform all administrative, fiscal and accounting procedures necessary to comply with contractual commitments, obligations regarding labor regulations, Social Security, etc.
- Manage payroll payments through banks.
- PD
- Work day registration
- Use CCTV for security purposes and to control employee's / collaborator's obligations.
- IT resources, email and internet access will be monitored to control employee's / collaborator's obligations and correct usage.
- Please note that the information obtained through CCTV may be used to impose disciplinary measures for breaching your duties and obligations as employee / collaborator.
- Manage other funds or social benefits as employee/collaborator.
- The Certificado Negativo de Penales (Criminal Record) is requested for purposes of complying with Spanish law.

To process your personal data for other purposes as specified under D below, your consent is required.

3. Your personal data will be stored while you are employee/collaborator of BFIS and in accordance with Spanish Statute of limitations.

Images recorded by CCTV are stored during 30 days, unless relevant incidents are recorded.

4. The lawful basis to process your personal data is: processing necessary to fullfill a contract, processing necessary to comply with the law, and your consent for other purposes as described under D.

5. Your personal data may be communicated to the following:

- Banks
- Spanish tax authorities
- Social Security and other entities from the Ministerio de Trabajo
- Inspección de Trabajo
- Entities that organize PD
- Unions for those employees/collaborators affiliated.
- Car rental companies
- Travel agencies, transportation companies, insurance companies, hotels, etc…
- Providers where communication is mandatory as per law.
- Entities that provide grants to BFIS
- Entities that organize PD and may be outside of the EU.

6. Your rights regarding processing of your personal data:

- Right of access
- Right to rectification
- Right to restrict processing where applicable
- Right to data portability
- Right to withdraw consent where applicable.

You may also lodge a complaint at the Spanish supervisory authority Agencia Española de Proteccion de Datos

Changes to your personal data must be communicated in writing to BFIS

7. BFIS will comply with GDPR should there be international data transfers involved of your personal data.

8. You are the source of your personal data. For students on internships at BFIS or external collaborators, the source of your data will also be the University where you are completing your studies or the Data Processor.

B - CONFIDENTIALITY AND DUTY OF SECRECY

All BFIS staff must:

1. Not disclose to third parties information and personal data they have Access to as employees/collaborators, except when disclosure is required by law.

2. Use the information described in the previous paragraph only to perform duties as BFIS employees/collaborators and not use it for any other purpose.

3. Not using information obtained as employee/collaborator not needed to perform duties and responsibilities as employee/collaborator

4. Comply with regulations on personal data processing, including but not limited to GDPR and Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

5. Confidentiality and duty of secrecy remain in full force and effect even after the employment/collaboration with BFIS is terminated.

In case of being a Trade Union Delegate or member of the Comité de Empresa, we inform you that the Estatuto de los Trabajadores establishes a duty of secrecy with respect to all information you have access to as Trade Union Delegate or member of the Comité de Empresa. This duty remains in full force and effect after your role as a Trade Union Delegate or member of the Comité de Empresa terminates.

C - SECURITY MEASURES AND AUTHORIZATIONS

The following security measures are mandatory for all BFIS employees / collaborators as per GDPR

1. Authorizations and Instructions

BFIS has appointed JOSEP PABLO as Security Officer. Regarding the Security Officer, employee/collaborator must:

- Follow instructions from the Security Officer related to systems, security measures, etc…
- Request authorization to use school owned devices, internet connection, etc…
- Request authorization as indicated in this document.

BFIS has appointed MIGUEL MARTINEZ HERNANDO as the Data Protection Officer DPO (dpo@bfischool.org). Regarding the DPO, employee/collaborator must:

- Answer information requests providing all information available regarding personal data processing and systems usage.
- Notify the DPO on new data processing activities before these take place.
- Notify technical and organizational changes that may have consequences on data processing activities or that may pose a risk on personal data being processed.
- Notify on new providers that may have access to or store personal data.
- Report data breaches and security incidents as described below.
- Notify on requests to exercise personal data rights.
- Notify on International Transfers of personal data that that take place outside of the European Economic Area (EEA)(international transfers of personal data take place when the Processor –provider- is located outside of the EEA)

2. All BFIS resources, including Internet connection and devices should be used for BFIS-purposes only and cannot be used for individual purposes.

BFIS may adopt all monitoring and control measures deemed necessary to verify compliance by the employee / collaborator with its obligations

The measures indicated above can be monitoring and tracking of browsing history, automatic alerts regarding email with attachments, monitoring and tracking of suspicious emails, and accessing emails if the employee is absent should this be necessary.

3. Incidents on personal data in documents/files and/ or devices shall be reported immediately to the Security Officer or the Data Protection Officer

4. Exercise of rights: requests to exercise rights by data subjects shall be forwarded immediately to the Security Officer or the Data Protection Officer.

5. Regarding paper documents/files (hard copies) from BFIS that the employee/collaborator has access to:

- Documents shall remain in custody to avoid them being seen, accessed or manipulated by third parties.
- Documents shall be kept/stored under lock and key. .
- Copies of said documents require a BFIS authorization
- Disposal of documents will require their destruction or shredding so as to prevent retrieving the information afterwards

With regards to Computer documents / e-files containing personal data, the employee/collaborator who created them and the employee/collaborator with permission to edit said files are responsible that no unauthorized disclosure or unauthorized access occur, placing them in restricted access units, configuring access / viewing permissions restrictively, limiting sharing options, and disabling options to download, print and copy.

6. Passwords provided to the employee / collaborator, will be renewed at least once a year, avoiding short or easy to guess passwords, and will be kept completely confidential, in no case will they be communicated to third parties or stored in visible places.

7. Installing apps, setting up coporate accounts and or reconfiguring BFIS computers, laptops and other devices requires authorization.

8. Storage devices (USB memory sticks or similar) require authorization from BFIS to be used.

9. Devices should be locked to prevent access by unauthorzed third parties.

10. Documents and IT devices leaving BFIS premises should be authorized by BFIS.

11. Temporary files should be deleted once the purpose for which they were created is completed.

12. Cloud computing services/file sharing is prohibited unless authorized by BFIS.

13. Using personal computers/devices for BFIS purposes: you must request a specific authorization to use your personal computer/device for BFIS purposes. When authorized, you must ensure the following:

- Computers and devices used by different users will have different users/profiles.
- Profiles with administration rights will be available for the installation and configuration of the operating system. This measure will prevent access privileges or modifying operating systems in the event of a cyber security attack.
- Passwords are mandatory to access personal data from BFIS
- Every user with access to personal data from BFIS must have a specific username and password.
- Computers and devices should be locked when inactive or when employee is not in front of them and a password required to unlock them.
- Passwords must be kept confidential. In no case will they be shared or exposed to third parties.
- All devices and computers used to store and process personal data should be updated on a regular basis.
- Operating system manufacturer's recommendations shall be followed regarding anti-virus software/systems.
- Firewalls should be activated whenever available
- If personal data is to be removed from the computer or device, either by physical means or by electronic means, an encryption method should be assessed to guarantee the confidentiality of personal data in case of improper access.
- A backup copy will be made periodically on a device other than the one used for regular work. The copy will be stored in a safe place, different from that in which the equipment is located with the original files, in order to allow recovering personal data should the information be lost.

14. All provisions of this document shall remain in full force and effect after employment / collaboration with BFIS is terminated.

15. The norms and protocols established in this document are part of the employee's employment obligations, and their breach may result in a disciplinary sanction, including dismissal, notwithstanding the fact that such conduct may be subject to criminal law.

Likewise, the worker / collaborator may be held liable to BFIS and third parties for any damage that may arise for breaching the rules established in this document. BFIS reserves the right to demand compensation for indemnities, sanctions or claims paid/satisfied by BFIS as a result of said breach.

D - CONSENT TO PROCESS PERSONAL DATA FOR PURPOSES NOT RELATED TO THE EMPLOYMENT/COLLABORATION RELATIONSHIP

Employee/Collaborator "gives/does not give" consent to the following:

YES	NO	
☐	☐	Use pictures on the BFIS website, directory, social media, magazines and other publications. Using pictures on social media might imply transfers of personal data outside of the European Economic Area.
☐	☐	Send birthday cards, or other cards to congratulate other relevant events like retirements, parenthood, etc… (sending these cards might disclose specific personal data such as birth date).
☐	☐	Use employeee's/collaborator cell phone number to communicate matters related to BFIS including data transfers regarding the use of apps and disclosing the cell phone number to other participants..
☐	☐	Transfer personal data to other companies/organizations that organize PD (they may be located outside of the EU).

By signing below I acknowledge that I have fully read and understood the contents of this document. I understand that if I have any questions, it is my responsibility to discuss them with the Data Protection Officer and/or the Security Officer

SIGNATURE:	-------- please complete and sign the Spanish language version --------
FULL NAME:	
DNI / NIE / PASAPORTE:	
FECHA	