POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

ESHOTUGEST, S.L. (VATEL ESPAÑA)

CONTROL DE VERSIONES		
EDICION	**FECHA**	**DESCRIPCIÓN**
Primera	10-4-2018	Se crea este documento para adaptar a VATEL a las previsiones del RGPD

ÍNDICE

1. INTRODUCCIÓN

La evolución tecnológica y la globalización han tenido incidencia directa en la privacidad y en la necesidad de proteger los datos personales. La magnitud de la recogida y del intercambio de estos ha aumentado exponencialmente en los últimos tiempos y el desarrollo de nuevas tecnologías ha hecho aparecer riesgos antes desconocidos. Todo ello exige que se impongan normas que garanticen la tutela de la privacidad y la protección de los datos personales

La presente **Política de Protección de Datos Personales** describe las normas y procedimientos que deben tenerse en cuenta en el tratamiento de dichos datos en ESHOTUGEST, S.L.-VATEL ESPAÑA, (En adelante, la Escuela o la Entidad) con objeto de garantizar el cumplimiento de la normativa aplicable en materia de protección de datos personales y poder demostrarlo.

En concreto, los objetivos de la presente de la presente **Política de Protección de Datos Personales** son:

- Indicar los principios y condiciones a los que debe sujetarse el tratamiento de datos de carácter personal en la Entidad. Precisar los supuestos en qué dicho tratamiento de datos es lícito y, por tanto, puede llevarse a cabo, y aquellos en los que no.
- Describir los deberes de información a los interesados que hay que observar en el tratamiento de sus datos personales.
- Informar sobre los requisitos que han de cumplirse cuando se vayan a poner datos personales a disposición de un tercero.
- Establecer qué derechos corresponden a los interesados titulares de los datos y el modo de atenderlos.
- Describir los mecanismos establecidos por la Entidad para cumplir con sus obligaciones, con el fin de que sean observados por todos los usuarios con acceso a datos personales.

2. NORMATIVA APLICABLE

- 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 datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos o RGPD).
- Ley Orgánica de Protección de Datos Personales.

3. DEFINICIONES

- **(i) Datos personales:** Toda información sobre una persona física identificada o identificable, considerándose tal toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular, mediante un identificador.

Son datos personales, por ejemplo, el nombre, apellidos, dirección (postal y electrónica), edad, estado civil, profesión, sexo, imagen, voz, o cualquier otro tipo de información que se encuentre vinculada a una persona física.

- **(ii) Tratamiento:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, por procedimientos automatizados o no, como, por ejemplo, la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

  Los tratamientos de datos se hacen, habitualmente, de forma automatizada, mediante programas informáticos que permiten crear y gestionar bases de datos. Pero también se pueden llevar a cabo tratamientos no automatizados, como los que se efectúan en papel (contratos, formularios médicos, nóminas, currículo vitae, etc.)

- **(iii) Fichero:** Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o repartido de forma funcional o geográfica. La Entidad utiliza ficheros para la gestión de sus actividades, incluyendo datos de alumnos, de sus responsables económicos, colaboradores-profesores, colaboradores-trabajadores, colaboradores-establecimientos hoteleros, turísticos, proveedores de servicios, interesados, etc.

- **(iv) Responsable del tratamiento:** La persona física o jurídica, autoridad pública, servicio u organismo que, sólo o junto con otros, determine los fines y medios del tratamiento.

  A efectos de la presente Política, el Responsable del Tratamiento es ESHOTUGEST, S.L. (VATEL ESPAÑA), cuyo principal objeto es las actividades docentes y de formación.

- **(v) Delegado de Protección de Datos o DPD:** Persona o empresa que asume la función de asesorar a la Entidad para el cumplimiento de la normativa sobre protección de datos personales. Es designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos.

  La Entidad debe garantizar que el DPD participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales, respaldándole, facilitando los recursos para el desempeño de dichas funciones, el acceso a los datos personales y a las operaciones de tratamiento, y el mantenimiento de sus conocimientos especializados.

  El DPD debe desarrollar sus funciones con absoluta independencia. No podrá recibir instrucciones en lo que respecta al desempeño de dichas funciones, no será destituido ni sancionado por su desempeño y rendirá cuentas directamente al más alto nivel jerárquico de la Entidad.

Es DPD de la Entidad está pendiente de designar en la fecha de este documento. Una vez sea designado, se deberán incluir en él su identidad y sus datos de contacto

En el caso de ESHOTRUGEST, S.L., no es obligatorio nombrar un DPD. No obstante, si la Entidad lo considera necesario podrá nombrarlo/a y se publicarán sus datos, al menos, en la página Web de la Entidad y se notificarán a la autoridad de control. Para esto último se utilizará el formulario que se incluye como **ANEXO I** a la presente **Política de Protección de Datos Personales**.

- **(vi) Encargado del tratamiento:** La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

  Es el caso de terceros proveedores que, como encargados del tratamiento, necesitan tratar los datos para prestar servicios a la Entidad (gestorías, hoteles, restaurantes y establecimientos turísticos, empresas informáticas, plataformas de internet etc.).

- **(vii) Destinatario:** La persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.

- **(viii) Tercero:** Persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

  Por ejemplo, es un tercero la entidad a la que se comunican datos personales del interesado para que sean tratados por esta con sus propios fines, en su caso.

- **(ix) Usuarios:** Todas las personas físicas que, de una manera u otra, presten servicios para el Responsable del Tratamiento como consecuencia de una relación contractual, de colaboración o de prestación de servicios y, como consecuencia de ello, realicen, traten, manipulen o, de cualquier manera, tengan acceso a datos de carácter personal de los que sea responsable la Entidad.

- **(x) Consentimiento de Personas Físicas:** Toda manifestación de voluntad libre, específica, informada e inequívoca por la que: estudiantes, responsables económicos, profesores, trabajadores, colaboradores, proveedores de servicios, interesados, etc., aceptan, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen.

- **(xi) Violación de la seguridad de los datos personales:** Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a los datos.

  Por ejemplo, si se produjese una incidencia informática (virus, hacker, etc.) que pusiese en peligro la confidencialidad, integridad o disponibilidad de los datos personales.

- **(xii) Autoridad de control:** Autoridad que tiene legalmente conferidas las facultades de supervisar el cumplimiento de la normativa sobre protección de datos y corregir las desviaciones que se produzcan. En el caso de España, la autoridad de control es la Agencia Española de Protección de Datos (AEPD).

- **(xiii) Colaborador:** Todas las personas físicas o jurídicas, que de una manera u otra colaboran con la ESCUELA para que esta desarrolle y pueda lograr su objeto social, entre ellos están: profesores, trabajadores, establecimientos donde los alumnos realizan sus prácticas, gestorías, etc.

- **(xiv) Estudiantes:** Todos los que cursan estudios en los distintos programas que se imparten en los centros docentes del Responsable del Tratamiento.

- **(xv) Responsables Económicos:** Las personas físicas que sufragan los estudios de los estudiantes.

- **(xvi) Proveedores de Servicios:** Todas las personas físicas o jurídicas que prestan algún tipo de servicio en virtud de una relación contractual con el Responsable del Tratamiento.

- **(xvii) Interesados:** Todas las personas físicas, que, por un medio u otro, contactan con el Responsable del Tratamiento, recabando información sobre sus programas de estudios y centros docentes.

4. ÁMBITO DE APLICACIÓN

4.1. Ámbito objetivo de aplicación.

La presente **Política de Protección de Datos Personales** es de aplicación al recabo y tratamiento de datos de personas físicas por la Entidad. Se excluyen los datos de personas jurídicas (sociedades mercantiles, instituciones, etc.) y los datos de personas fallecidas.

El tratamiento puede ser realizado automatizadamente o en papel. No obstante, en este último caso, esta **Política de Protección de Datos Personales** sólo es aplicable si los datos en papel están contenidos en un fichero o destinados a ser incluidos en él.

4.2. Ámbito subjetivo de aplicación.

La presente **Política de Protección de Datos Personales** es obligatoria para todas aquellas personas que reúnan las siguientes condiciones:

- Que se encuentren vinculadas a la Entidad mediante contrato de servicios, laboral o mercantil, relaciones de colaboración, acuerdo o contrato de formación (programas de Bachelor y MBA, prácticas, ampliación de estudios y cualquier otro que tenga por objeto su formación, etc.), interesados en los programas de estudios de la Escuela o, en general, cualquier otro tipo de relación jurídica análoga, verbal o escrita.

- Que, en el cumplimiento de sus funciones y obligaciones, dispongan de acceso autorizado a los equipos, sistemas, redes de comunicación interna y externa, herramientas, aplicaciones o programas integrantes del Sistema de Información de la Entidad o a documentación en papel en la que consten datos personales.

A efectos de esta **Política de Protección de Datos Personales**, dichas personas serán denominadas "usuarios".

5. ACTIVIDADES DE TRATAMIENTO PERMITIDAS

En el **ANEXO II** de esta **Política de Protección de Datos Personales** se incluyen las actividades de tratamiento de datos que están autorizadas en la Entidad. Los usuarios no podrán llevar a cabo actividades de tratamiento de datos personales diferentes de las indicadas o fuera de los límites previstos en dicho **ANEXO II.**

Si un usuario considerase necesario iniciar una actividad de tratamiento de datos personales distinta de las contempladas en el **ANEXO II** o modificar alguna de las existentes, lo notificará con carácter previo al DPD, mediante correo electrónico, y no iniciará la nueva actividad de tratamiento hasta que reciba confirmación de que puede hacerlo. En defecto de DPD, se consultará al Responsable de Seguridad de la empresa a efectos del SGSI.

Siempre que se inicien actividades de tratamiento, distintas de las comprendidas en el **ANEXO II** o se modifiquen las ya existentes, se deberá realizar un Registro de Actividades de Tratamiento. Se incluye en esta obligación los servicios que se presten a los clientes con acceso a sus bases de datos de carácter personal; deberá elaborarse un Registro de Actividades para cada uno de estos tratamientos de datos.

El Registro de Actividades de Tratamiento actualizado se dará a conocer a todos los usuarios de la Entidad por el procedimiento que esta determine (circular interna, publicación en intranet, etc.).

6. REGLAS GENERALES PARA EL TRATAMIENTO DE DATOS PERSONALES

6.1. Principios relativos al tratamiento de datos personales.

Cualquier tratamiento de datos personales debe cumplir los siguientes principios:

a) **Licitud, lealtad y transparencia:** Los datos serán tratados de manera lícita, leal y transparente en relación con el interesado.

b) **Limitación de la finalidad:** Los datos serán recogidos con fines determinados, explícitos y legítimos, y no tratados ulteriormente de manera incompatible con dichos fines.

c) **Minimización de datos:** Los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

d) **Exactitud:** Los datos serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

e) **Limitación del plazo de conservación:** Los datos serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento.

f) **Integridad y Confidencialidad:** Los datos serán tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

La Entidad es legalmente responsable de que se cumplan dichos Principios. Para poder demostrar su cumplimiento, se adoptarán proactivamente las medidas que se indicarán más adelante.

6.2. Licitud del tratamiento de datos personales.

Sólo podrán tratarse datos personales si se da alguna de las siguientes circunstancias:

a) Que el interesado haya dado su **consentimiento** explícito para el tratamiento con uno o varios fines específicos. Este consentimiento debe poder demostrarse. Se podrá retirar el consentimiento en cualquier momento, por un medio que sea, al menos, tan sencillo como el utilizado para obtenerlo.

b) Que el tratamiento sea necesario para la **ejecución de un contrato** en el que el interesado sea parte o para la aplicación, a petición de este, de medidas precontractuales.

c) Que el tratamiento sea necesario para el cumplimiento de una **obligación legal** por la Entidad o para el ejercicio de **poderes públicos** que tenga conferidos, en su caso.

d) Que el tratamiento sea necesario para la satisfacción de **intereses legítimos** perseguidos por la Entidad o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. La aplicación de este supuesto exigirá la previa ponderación de dichos intereses, lo cual deberá decidirse sólo con intervención y asesoramiento del DPD. En defecto de DPD, se consultará a un asesor experto en protección de datos.

6.3. Tratamiento de categorías especiales de datos personales.

Queda prohibido el tratamiento por la Entidad de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca

a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

Los datos aportados en formulario que el personal médico seleccionado por los alumnos, certifique algún tipo de enfermedad o padecimiento físico o psíquico, serán recogidos, tratados y archivados en formato papel. AS los que

Dicha prohibición no será aplicable en determinados casos, entre otros, si las personas físicas dieron su consentimiento explícito (y puede demostrarse), si se trata de datos personales que los mismos han hecho manifiestamente públicos, si el tratamiento es necesario para el cumplimiento de obligaciones y derechos en el ámbito docente, formativo, laboral y de la seguridad y protección social o si el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad del alumnos para realizar sus prácticas en los diferentes establecimientos hoteleros, de hostelería y turísticos en general, profesores y trabajadores, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social.

El tratamiento de datos personales relativos a condenas e infracciones penales sólo es posible cuando lo autorice la normativa aplicable.

7. OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

7.1. Aplicación de medidas técnicas y organizativas adecuadas.

La Entidad está obligada a aplicar medidas técnicas y organizativas apropiadas para poder garantizar y demostrar el cumplimiento de sus obligaciones en materia de protección de datos.

Las medidas adoptadas se revisarán y actualizarán, al menos, una vez al año.

7.2. Privacidad desde el diseño y por defecto.

Siempre que se diseñen o inicien nuevas actividades de tratamiento de datos, se deben aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas concebidas para aplicar de forma efectiva los principios de protección de datos (como la seudonimización o la minimización de datos) e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos legales y proteger los derechos de los interesados.

Asimismo, se aplicarán las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas físicas.

A los efectos de cumplir los referidos principios, se deberá consultar siempre al DPD o, en su defecto, a un asesor experto en protección de datos.

7.3. Información a las personas físicas sobre el recabo de sus datos personales.

En el momento de recabar los datos, debe informarse a las personas físicas de las condiciones en las que serán tratados y de los derechos legales que les asisten. Dicha información debe realizarse por escrito, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

También debe cumplirse ese deber en caso de que los datos no hayan sido recabados de las personas, sino de un tercero. En este caso, la información debe hacerse, a más tardar, en el plazo de un mes, o, si los datos han de utilizarse para comunicación con dichas personas, a más tardar en el momento de la primera comunicación a dicha persona, o, si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

Para el cumplimiento de los deberes de información, se utilizarán las cláusulas informativas y de confidencialidad que constan en los **ANEXOS III, IV, V, VI, VII, VIII**, así como la cláusula informativa de los formularios de la citada web, que consta como **ANEXO IX**, de esta **Política de Protección de Datos Personales**, en la forma indicada para cada una de ellas.

7.4. Prestaciones de servicios con acceso a datos.

En ocasiones, se contrata a encargados del tratamiento para prestar a la Entidad servicios que implican la necesidad de realizar tratamientos de datos por cuenta de esta.

En estos casos, se deberán elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos legales y garantice la protección de los derechos del interesado.

Dichas garantías han de exigirse al encargado mediante la firma del contrato que se incluye en el **ANEXO XI** de esta **Política de Protección de Datos Personales**.

Igualmente, debe firmarse con el cliente el correspondiente contrato cuando la Entidad, para prestar servicios a aquel, necesite acceder a sus bases de datos personales. En caso de subcontratación de dichos servicios, la Entidad debe también firmar el correspondiente contrato con el subcontratista.

La Dirección de la Entidad será responsable de velar por que dichos contratos se firmen en todos los casos en que sea necesario. En caso de duda, se consultará al DPD, o, en su defecto, a un asesor experto en protección de datos.

7.5. Seguridad de los datos.

7.5.1 Aplicación de medidas técnicas y organizativas.

La Entidad, en función de los riesgos que se han detectado y que constan en el pertinente Análisis de Riesgos, debe aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Tales medidas son las que se incluyen en el Documento de de Seguridad, que se incluye como **ANEXO XII.** Tanto la Entidad como todos los usuarios están obligados a cumplir dichas medidas.

7.5.2 Notificación de violaciones de la seguridad de los datos personales.

En aquellos casos en que se detecte una violación de la seguridad que ponga o haya podido poner en peligro la confidencialidad, integridad o disponibilidad de los datos personales tratados por la Entidad, dicha quiebra de seguridad deberá ser gestionada y, en su caso, notificada a la AEPD o a los interesados.

Para la gestión, registro y, en su caso, notificación de violaciones de la seguridad, se aplicará el procedimiento que se incluye como **ANEXO XIII**.

7.6. Deber de secreto.

La Entidad, todos los usuarios y personas físicas que accedan a los datos de carácter personal deben guardar secreto sobre ellos, aún después de finalizar la relación en cuya virtud conocieron los datos, ya sea laboral o de cualquier otro tipo.

A tal fin, los usuarios y personas físicas deberán firmar el documento de información, consentimiento y confidencialidad, cuyos modelos se incluyen en los **ANEXOS III, IV, V, VI, VII, VIII y IX**, debiendo firmar el modelo incluido en el número **III**), los alumnos y sus responsables económicos, en el del número **IV**), los alumnos menores de 18 años de edad y mayores de 16, en el del número **V)**, los colaboradores-profesores, en el del número **VI**), los colaboradores-trabajadores, en el del número **VII**), los colaboradores en general, entre ellos, los establecimientos hoteleros, turísticos y de hostelería donde los estudiantes realizan sus prácticas, gestorías etc., en el del número **VIII**), proveedores de servicios que tienen relación con la ESCUELA, en el del número **IX)**, los interesados que solicitan información a la ESCUELA mediante los formularios que se encuentran publicados en la página web de esta.

7.7. Cooperación y gestión de relaciones con la autoridad de control.

La Entidad debe cooperar con la autoridad de control (AEPD), si esta se lo solicita en el desempeño de sus funciones.

Siempre que se reciba una solicitud, requerimiento o comunicación de la autoridad de control (AEPD), se pondrá en conocimiento del DPD o de la Dirección de la Entidad por escrito y de forma inmediata, para que éstos la respondan o den las pautas oportunas para dicha respuesta. En defecto de DPD, se consultará a un asesor experto en protección de datos.

7.8. Transferencias internacionales de datos.

La transferencia de datos personales fuera del Espacio Económico Europeo exige el cumplimiento de determinadas condiciones legales. Esta regla es aplicable también en aquellos casos en los que, por utilizarse servicios en la nube o fórmulas similares, los servidores en los que se alojan o tratan dichos datos no se encuentran, total o parcialmente, dentro del Espacio Económico Europeo o los datos viajan fuera de este.

A tal fin, siempre que se prevean realizar tratamientos de datos personales que impliquen su transferencia internacional, se pondrá previamente y por escrito en conocimiento del DPD, quien dará las pautas oportunas para que dicha transferencia pueda cumplir la normativa aplicable. La transferencia internacional de datos no se efectuará hasta que el DPD confirme que se cumplen las condiciones exigidas por dicha normativa. En defecto de DPD, se consultará a un asesor experto en protección de datos.

7.9. Evaluación de impacto relativa a la protección de datos.

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas, se debe realizar previamente una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

Para ello, siempre que se vaya a realizar un nuevo tratamiento de datos personales o se vaya a modificar de forma sustancial uno de los ya existentes, se pondrá previamente y por escrito en conocimiento del DPD, a los efectos de que este asesore sobre la necesidad o no de realizar una evaluación de impacto relativa a la protección de datos y sus condiciones. En defecto de DPD, se consultará a un asesor experto en protección de datos.

8. EJERCICIO DE DERECHOS POR LOS INTERESADOS

8.1. Derechos reconocidos a los interesados.

La normativa aplicable reconoce a los interesados los siguientes derechos:

a) Acceso.- Es la facultad de obtener información sobre si la Entidad está tratando o no sus datos personales y, en tal caso, conocer qué datos son, los fines para los que se tratan, los terceros a los que se hayan comunicado, el plazo de conservación previsto y otras informaciones relevantes.

b) Rectificación.- Es el derecho a la corrección de sus datos personales, cuando sean inexactos, y a completarlos, cuando sean incompletos.

c) Supresión.- Es la facultad de obtener la eliminación de sus datos personales cuando ya no sean necesarios para los fines para los que fueron recogidos, o cuando el interesado haya retirado el consentimiento para tratar los datos, se oponga a dicho tratamiento en base a su situación personal, los datos se estén tratando ilícitamente o concurra alguno de los restantes supuestos legales.

d) Oposición.- Es el derecho a negarse en cualquier momento, por motivos relacionados con su situación particular, a que sus datos personales sean tratados en base a la existencia de un interés legítimo.

e) Negativa a ser sometido a decisiones individuales automatizadas.- Es el derecho a negarse a ser objeto de una decisión basada únicamente en el tratamiento

automatizado de sus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

f) Limitación del tratamiento.- Es el derecho a que los datos no sean tratados por la Entidad temporalmente o lo sean de forma limitada, en los siguientes supuestos:

   i) Cuando el interesado haya impugnado su exactitud, durante el plazo en que la Entidad pueda verificar dicha exactitud.

   ii) Cuando el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos y solicite en su lugar la limitación de su uso.

   iii) Cuando la Entidad ya no necesite los datos personales, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

   iv) Cuando el interesado se haya opuesto al tratamiento en base a sus circunstancias personales, mientras se verifica si los motivos legítimos de la Entidad prevalecen sobre los del interesado.

   En todos estos casos, los datos sólo podrán ser conservados, pero no tratados para otros fines, salvo consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, la protección de los derechos de terceros o por razones de interés público.

g) Portabilidad.- Es el derecho a recibir sus datos personales, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento.

8.2. Obligaciones en relación con el ejercicio de derechos.

La Entidad debe facilitar gratuitamente el ejercicio de derechos de los interesados y darles respuesta por escrito y en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. Cuando la solicitud se presente por medios electrónicos, la información se facilitará por esos mismos medios, salvo que el interesado solicite otro medio.

La respuesta debe remitirse en el plazo máximo de un mes a partir de la recepción de la solicitud, tanto si se admite esta, como si no, informando en este último caso, además, de la posibilidad de presentar una reclamación ante la autoridad de control (AEPD) y ejercer acciones judiciales.

Cualquier rectificación, supresión o limitación del tratamiento de datos personales efectuada debe notificarse a cada uno de los destinatarios a los que se hayan comunicado los datos, salvo que sea imposible o exija un esfuerzo desproporcionado. Se informará al interesado acerca de dichos destinatarios, si este así lo solicita.

8.3. Procedimiento de respuesta al ejercicio de derechos.

Cuando cualquier usuario reciba una solicitud de ejercicio de derechos, por cualquier vía, debe trasladarla por escrito al DPD, a la mayor brevedad, para que este proceda a su tramitación o dé las pautas necesarias para ello. En defecto de DPD, se consultará a un asesor experto en protección de datos.

8.4. Plazos que establecen para tratar los datos.

Con carácter general, a título enunciativo y sin perjuicio de cualesquiera otros plazos que puedan estar previstos en otras normas o circulares y que resulten igualmente de aplicación, cabe hacer mención a los siguientes plazos durante los cuales será necesario conservar los datos personales que hubiesen sido objeto de tratamiento:

- 15 años para los datos de ALUMNOS, RESPONSABLES ECONOMICOS, COLABORADORES-TRABAJADORES, COLABORADORES- PROFESORES y PROVEEDORES DE SERVICIOS, salvo que sea aplicable un plazo inferior de conservación. Este plazo se corresponde con el general establecido para la prescripción de las acciones personales en la legislación civil.

- 6 años para los datos de COLABORADORES, PROVEEDORES DE SERVICIOS, INTERESADOS y SUMINSTRADORES, en lo que se refiere al cumplimiento de la obligación de conservar libros, correspondencia, documentación y demás justificantes concernientes a su negocio.

- 5 años para los datos de clientes y proveedores, en lo que se refiere al cumplimiento de obligaciones de pago que deban hacerse por años o plazos más breves. Datos relativos al cumplimento de obligaciones en materia de Prevención de Riesgos Laborales y sobre Infracciones y Sanciones en el Orden Social.

-4 años para los datos relativos al cumplimiento de la obligación de pago de las cuotas de la Seguridad Social de los trabajadores.

- 3 años para los datos contenidos en los registros de accesos ("logs") a los datos de nivel de seguridad alto contenidos en las aplicaciones informáticas de la ESCUELA.

- 1 año para las restantes categorías de datos de trabajadores. Es decir, los datos relativos a la relación laboral deberán conservarse, al menos, hasta que transcurra un año desde la expiración del contrato, como regla general.

- 30 días para los datos recabados en los registros de visitas de acceso a edificios, a contar desde el día en que fueron recabados. Y 30 días si se recaban imágenes con los sistemas de videovigilancia, a contar desde el día en que fueron recabados.

9. TRATAMIENTO DE DATOS PERSONALES CON FINES DE VIGILANCIA MEDIANTE CÁMARAS O VIDEOCÁMARAS.

El tratamiento de datos personales, en especial imágenes, como resultado del uso de cámaras de vigilancia se somete a ciertas reglas propias.

9.1. Calidad de los datos.

Sólo podrán utilizarse cámaras de vigilancia cuando ésta no pueda llevarse a cabo por otros medios menos intrusivos para la intimidad, siempre que estos otros medios no exijan esfuerzos desproporcionados.

Las cámaras no podrán obtener imágenes de espacios públicos, salvo que sea imprescindible para la vigilancia o resulte imposible evitarlo por su ubicación.

Los datos personales grabados por las cámaras de videovigilancia deben ser cancelados en el plazo máximo de un mes desde su obtención.

9.2. Información.

En caso de colocarse cámaras de vigilancia, deben adoptarse las dos medidas siguientes:

- Colocar en cada uno de los accesos a las zonas vigiladas un distintivo informativo suficientemente visible, tanto en espacios abiertos como cerrados. En el **ANEXO XIV** se encuentran los modelos de dichos distintivos. Se incluyen dos modelos diferentes, debiendo utilizarse uno u otro según existan cámaras de vigilancia o meros sistemas de alarma con grabación de imágenes.

- Poner a disposición del público los impresos cuyos modelos constan en el **ANEXO XVI**. De los tres modelos que se incluyen, se deberá utilizar uno u otro según las cámaras graben las imágenes permanentemente, sólo graben las imágenes cuando se active la alarma o no graben y se limiten a reproducir las imágenes en tiempo real. Se recomienda que los impresos se pongan a disposición del público en algún mostrador o mesa accesible dentro de la zona videovigilada.

9.3. Condiciones exigibles a la empresa instaladora.

a) Sistemas de Videovigilancia conectados a una central de alarmas.

Su instalación y mantenimiento sólo pueden hacerse por empresas de seguridad privada, autorizadas para ello por el Ministerio del Interior. Con dicha empresa ha de firmarse un contrato escrito que aquella debe notificar a dicho Ministerio.

La Entidad debe comprobar que la empresa reúne dichas exigencias. Para ello, debe solicitarle que aporte copias de los documentos que lo acrediten y firmar con ella el modelo de contrato que se adjunta en el **ANEXO XII**

b) Sistemas de Videovigilancia no conectados a una central de alarmas.

Si el sistema no se encuentra conectado a una central de alarmas, su instalación y mantenimiento pueden hacerse por cualquier particular o empresa, si bien debe firmarse con esta el modelo de contrato que se incluye en el en el **ANEXO XII**.