

3. Otras disposiciones

UNIVERSIDADES

RESOLUCIÓN de 13 de diciembre de 2012, de la Universidad de Granada, por la que se ordena la publicación del Reglamento de Protección de Datos de Carácter Personal.

Conforme a lo acordado por el Consejo de Gobierno de la Universidad de Granada de 4 de diciembre de 2012,

D I S P O N G O

1. Ordenar la publicación, en el Boletín Oficial de la Junta de Andalucía, del Reglamento de Protección de Datos de Carácter Personal de la Universidad de Granada.

2. El presente Reglamento de Protección de Datos de Carácter Personal de la Universidad de Granada tendrá efectos a partir del día siguiente de su publicación en el Boletín Oficial de la Universidad de Granada (BOUGR) sin perjuicio de su publicación en el Boletín Oficial de la Junta de Andalucía.

Granada, 13 de diciembre de 2012.- El Rector, Francisco González Lodeiro.

REGLAMENTO DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE LA UNIVERSIDAD DE GRANADA

(Aprobado en sesión ordinaria de Consejo de Gobierno de 4 de diciembre de 2012)

Í N D I C E

PREÁMBULO

CAPÍTULO PRIMERO. Disposiciones generales.

Artículo 1. Objeto.

Artículo 2. Ámbito de aplicación.

Artículo 3. Confidencialidad y seguridad.

CAPÍTULO SEGUNDO. Obligaciones previas al tratamiento de datos de carácter personal.

Artículo 4. Procedimiento de creación, modificación y supresión de ficheros.

CAPÍTULO TERCERO. Recogida de datos de carácter personal.

Artículo 5. Modo de recabar los datos.

Artículo 6. Calidad en la recogida de los datos.

Artículo 7. Información sobre el tratamiento

Artículo 8. Consentimiento para el tratamiento.

Artículo 9. Datos especialmente protegidos.

CAPÍTULO CUARTO. Usos y finalidades del tratamiento.

Artículo 10. Calidad en el uso de los datos.

Artículo 11. Acceso a datos por cuenta de terceros.

CAPÍTULO QUINTO. Régimen de cesión de datos de carácter personal.

Artículo 12. Consentimiento para la cesión.

Artículo 13. Datos especialmente protegidos.

Artículo 14. Obtención del consentimiento.

Artículo 15. Procedimiento de cesión de datos.

Artículo 16. Cesiones de datos a autoridades judiciales y administrativas especiales.

CAPÍTULO SEXTO. Fin del tratamiento.

Artículo 17. Calidad de los datos en la cancelación.

CAPÍTULO SÉPTIMO. Derechos de los interesados.

Artículo 18. Requisitos Generales.

Artículo 19. Derecho de acceso.

- Artículo 20. Derechos de rectificación y cancelación.
- Artículo 21. Derecho de oposición.
- Artículo 22. Denegación de los derechos.
- Artículo 23. Procedimiento Interno de Tramitación.

CAPÍTULO OCTAVO. Videovigilancia.

- Artículo 24. Ámbito objetivo.
- Artículo 25. Principios de calidad, proporcionalidad y finalidad del tratamiento.
- Artículo 26. Información.
- Artículo 27. Derechos de acceso, rectificación, cancelación y oposición.
- Artículo 28. Cancelación de los datos.
- Artículo 29. Seguridad y confidencialidad.

CAPÍTULO NOVENO. Funciones y obligaciones de las figuras responsables.

- Artículo 30. Responsable del fichero.
- Artículo 31. Designación de Responsables.
- Artículo 32. Funciones y obligaciones de la Secretaría General.
- Artículo 33. Funciones y obligaciones del Responsable de Seguridad.
- Artículo 34. Funciones y obligaciones del Coordinador LOPD.
- Artículo 35. Funciones y obligaciones de los usuarios.

DISPOSICIONES ADICIONALES.

- Disposición adicional primera. Actuaciones ante la Agencia Española de Protección de Datos.
- Disposición adicional segunda. Denominación de género.

DISPOSICIÓN TRANSITORIA.

DISPOSICIONES FINALES.

- Disposición final primera. Instrucciones de desarrollo.
- Disposición final segunda. Medidas técnicas de seguridad de carácter centralizado.
- Disposición final tercera. Entrada en vigor.

ANEXO I. Definiciones.

ANEXO II. Cláusula informativa para la recogida y cesión de datos de carácter personal.

ANEXO III. Formulario para recabar el consentimiento para la recogida y cesión de datos de carácter personal.

ANEXO IV. Modelos de cláusula de protección de datos de carácter personal y medidas de seguridad y de acuerdo de confidencialidad para el tratamiento de datos de carácter personal y medidas de seguridad.

P R E Á M B U L O

Desde la entrada en vigor de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal, derogada por la norma actualmente vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y especialmente a raíz de la entrada en vigor de su Reglamento de desarrollo, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre, la Universidad de Granada ha llevado a cabo un proceso de adecuación de sus procedimientos y concienciación de los miembros de la comunidad universitaria en el respeto al derecho fundamental a la protección de datos.

Por este motivo, la Universidad considera oportuno dictar un Reglamento que recopile y dé forma a la experiencia adquirida en estos años en el tratamiento de datos de carácter personal, tanto automatizados como no automatizados, y establezca unas pautas de actuación en el ámbito universitario que permitan conjugar el creciente desarrollo de las tecnologías de la información y las comunicaciones con el respeto a la privacidad de las personas físicas y el tratamiento de sus datos de carácter personal.

El presente Reglamento contiene cuatro Anexos, que incluyen, respectivamente: definiciones; cláusula informativa para la recogida y cesión de datos de carácter personal; formulario para recabar el consentimiento para la recogida y cesión de datos de carácter personal; modelo de cláusula de tratamiento de datos de carácter personal y medidas de seguridad para incluir en los Pliegos de Cláusulas Administrativas Particulares y, cuando los pliegos no sean aplicables, en los contratos de prestación de servicios que se suscriban con terceros; modelo de acuerdo de confidencialidad para el tratamiento de datos de carácter personal y medidas de seguridad para añadir a los contratos de prestación ya suscritos.

En su virtud, el Consejo de Gobierno, en sesión ordinaria celebrada el 4 de diciembre de 2012, aprueba el siguiente Reglamento:

CAPÍTULO PRIMERO

Disposiciones generales

Artículo 1. Objeto.

El presente Reglamento tiene por objeto regular en el ámbito de la Universidad de Granada los sistemas, medios y procedimientos que permitan, de la manera más eficaz, la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), así como su Reglamento de desarrollo aprobado por Real Decreto 1720/2007 (en adelante RDLOPD), en lo que se refiere al régimen jurídico aplicable a los ficheros de titularidad pública.

Artículo 2. Ámbito de aplicación.

Este Reglamento es de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de dichos datos en el ámbito y entorno de la Universidad de Granada, con motivo de las actividades en las que intervenga en cumplimiento de sus funciones como Administración Pública.

Este Reglamento no será aplicable a los tratamientos referidos a:

- a) Las personas jurídicas.
- b) Las personas físicas de contacto de personas jurídicas, consistentes únicamente en su nombre y apellidos, las funciones o puestos que desempeñen, dirección postal o electrónica, teléfono y número de fax profesionales.
- c) Los empresarios individuales, cuando se haga referencia a ellos en su calidad de comerciantes, industriales o navieros.
- d) Los profesionales autónomos, cuando tengan su actividad organizada como una empresa ostentando la condición de comerciante.

Artículo 3. Confidencialidad y seguridad.

1. El presente Reglamento establece las distintas obligaciones que deben ser respetadas por los usuarios de datos de carácter personal en la Universidad de Granada, en cada una de las fases del tratamiento de datos de carácter personal, teniendo la confidencialidad y la seguridad un carácter transversal, por lo que deberán ser tenidas en cuenta en todo momento.

2. En tanto la documentación que contenga datos de carácter personal no se incorpore en los dispositivos de almacenamiento, sean físicos o electrónicos, por encontrarse en proceso de trámite, la persona encargada de la mencionada documentación será responsable de su custodia.

3. El deber de secreto profesional respecto de los datos de carácter personal subsistirá incluso una vez finalizada la relación del usuario con la Universidad de Granada.

4. La Universidad adoptará las medidas necesarias para garantizar la seguridad de los datos de carácter personal, que estarán establecidas en un Documento de Seguridad, y dará a conocer al personal las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento, mediante la publicación en la página web de la Universidad de Granada de una Guía básica sobre Protección de Datos.

CAPÍTULO SEGUNDO

Obligaciones previas al tratamiento de datos de carácter personal

Artículo 4. Procedimiento de creación, modificación y supresión de ficheros.

1. La aprobación de la creación, modificación o supresión de ficheros de la Universidad de Granada corresponde al Rector mediante resolución publicada en el Boletín Oficial de la Junta de Andalucía (BOJA) y deberá ser notificada, en el plazo de un mes desde su publicación, a la Agencia Española de Protección de Datos o, en su caso, autoridad de control autonómica, a efectos de su inscripción en el Registro de Protección de Datos correspondiente.

2. La creación, modificación y supresión de ficheros será tramitada por la Secretaría General.

3. Cuando una Unidad de la Universidad, por razones de su competencia, necesite realizar un tratamiento de datos con una estructura distinta a la que figura en los ficheros registrados por la Universidad de Granada, solicitará a la Secretaría General la creación o modificación del fichero mediante escrito motivado. En caso de estimarse su procedencia, la Secretaría General llevará a cabo las actuaciones procedimentales de cara a la inscripción de un nuevo fichero o a la modificación de los ya existentes, según proceda.

Las modificaciones en la estructura del tratamiento podrán ser causadas, con carácter alternativo o acumulativo, por la necesidad de recabar datos, bien distintos a los empleados hasta ese momento, bien con

finalidades diferentes a las habitualmente desarrolladas o de otros colectivos distintos a aquellos de los que se hubiese requerido información hasta el momento o, en su caso, cuando se deban realizar nuevas cesiones o transferencias internacionales de datos de carácter personal.

4. Una vez que haya concluido la finalidad para la que se recabaron los datos y no vayan a ser objeto de tratamiento ulterior, deberá ser comunicado a la Secretaría General motivadamente con el objeto de que ésta inicie los trámites para la supresión del fichero correspondiente en el Registro de Protección de Datos.

5. No se podrá recabar ningún dato de carácter personal si no se encuentra previamente incluido en un fichero publicado y comunicado a la Agencia Española de Protección de Datos.

6. Recabar datos distintos o con finalidades distintas a los contenidos en los ficheros registrados sin contar con la previa autorización de la Secretaría General, o recabarlos con anterioridad a la publicación y comunicación a la Agencia Española de Protección de Datos de los ficheros, podrá dar lugar, en su caso, a responsabilidades disciplinarias, respondiendo el usuario frente a terceros y frente a la propia Universidad.

CAPÍTULO TERCERO

Recogida de datos de carácter personal

Artículo 5. Modo de recabar los datos.

La recogida de los datos de carácter personal en la Universidad de Granada se realizará para fines determinados, explícitos y legítimos, no pudiendo recogerse por medios fraudulentos, desleales o ilícitos.

Artículo 6. Calidad en la recogida de los datos.

1. Los datos recabados deben ser adecuados, pertinentes y no excesivos en relación con la finalidad para la cual hayan sido requeridos.

2. Los datos recabados en la Universidad de Granada deberán servir a fines directamente relacionados con sus competencias y funciones.

Artículo 7. Información sobre el tratamiento.

1. Siempre que se proceda a la recogida de datos de carácter personal directamente del interesado, se le facilitará la siguiente información:

a) La existencia de un tratamiento de datos de carácter personal, la finalidad de la recogida de éstos y los destinatarios de la información.

b) La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

c) La identificación y dirección de la Universidad de Granada, como responsable del Fichero.

2. Siempre que sea posible, se emplearán formularios o cuestionarios que incorporen dicha información para su cumplimentación, firma y entrega por parte del interesado, ya sea en papel o por correo electrónico, o a través de la página web con su aceptación, de forma que quede constancia del cumplimiento de dicha obligación. En otro caso y cuando proceda, la información deberá ser incluida en correos electrónicos de contestación, carteles informativos o en locuciones telefónicas, para lo que deberán elaborarse procedimientos que puedan ser auditados.

3. Cuando la aportación de algún dato por el interesado sea voluntaria, no considerándose imprescindible para alcanzar la finalidad que se pretende, se le deberá indicar señalando expresamente los campos obligatorios.

4. Si los datos se recaban de un tercero distinto del interesado, éste deberá ser informado, además de los extremos indicados, de la procedencia de los datos. Dicha información deberá facilitarse de forma expresa, precisa e inequívoca, dentro de los tres meses siguientes a la recogida de los datos.

5. El texto informativo que se adjunta en el Anexo II de este Reglamento, debidamente adaptado a las circunstancias de cada caso, debe ser insertado en todos los formularios o cuestionarios de recogida de datos, o en todo caso facilitado al interesado, todo ello sin perjuicio de lo establecido en el artículo 5.5 de la LOPD.

Artículo 8. Consentimiento para el tratamiento.

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado. El consentimiento podrá ser recabado por medios electrónicos que garanticen la identificación del interesado. A tal efecto, se incluyen entre ellos el correo electrónico corporativo para el personal y estudiantado de la Universidad de Granada y cualquier correo electrónico que el interesado hubiese indicado como medio de comunicación o notificación en el procedimiento administrativo de referencia.

2. No será preciso el consentimiento para el tratamiento cuando:

a) Una norma con rango de Ley o una norma de Derecho comunitario lo autorice, bien porque el tratamiento tenga por objeto satisfacer un interés legítimo de la Universidad amparado en dicha norma, cuando

no prevalezca el interés o los derechos y libertades de los interesados, o bien porque sea necesario para que la Universidad cumpla un deber que le impone dicha norma.

b) Los datos se recojan para el ejercicio de las funciones propias de la Universidad en el ámbito de las competencias que le atribuye la normativa universitaria.

c) Los datos se recaben con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el interesado y sean necesarios para su mantenimiento o cumplimiento.

d) Tenga por finalidad proteger un interés vital del interesado, resultando el tratamiento necesario para la prevención o el diagnóstico médicos, o la gestión de servicios sanitarios, realizados por un profesional sanitario u otra persona sujeta a una obligación equivalente de secreto profesional.

e) Los datos figuren en fuentes accesibles al público, de acuerdo con la definición contenida en el Anexo I, letra n) del presente Reglamento, y su tratamiento sea necesario para la satisfacción del interés legítimo de la Universidad, en cuyo caso no podrán facilitarse a entidades privadas, salvo con el consentimiento del interesado o que una Ley establezca algo distinto.

3. El consentimiento podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. No podrán establecerse para la revocación del consentimiento más requisitos que aquellos que se establecieron para solicitarlo, debiendo tener en todo caso carácter gratuito.

La revocación del consentimiento será solicitada ante la Secretaría General y, en caso de que proceda, conllevará el cese del tratamiento en un plazo no superior a diez días desde la recepción de la solicitud, debiendo ser confirmada al interesado únicamente en el caso en que éste lo hubiese requerido.

4. El consentimiento debe de ser además informado, por lo que podrá emplearse el texto informativo indicado en el artículo anterior, convenientemente adaptado. Dicho texto podrá referirse a un tratamiento o a una serie de ellos, siempre que se concreten y delimiten claramente las finalidades para las que son recabados los datos.

Cuando las distintas finalidades no guarden relación directa con el mantenimiento, desarrollo o control de la relación administrativa o contractual iniciada con la solicitud, se deberá permitir al afectado que manifieste su negativa al tratamiento mediante la marcación de una casilla claramente visible y que no esté premarcada, o estableciendo un procedimiento equivalente.

5. Corresponde a la Universidad acreditar que ha obtenido el consentimiento de los interesados. Para ello, en el Anexo III se incluye el modelo para recabar el consentimiento para la recogida y cesión de datos de datos de carácter personal.

Artículo 9. Datos especialmente protegidos.

1. La recogida de datos relativos a ideología, religión, creencias y afiliación sindical, requiere consentimiento expreso y por escrito del interesado, debiendo ser advertido de su derecho a no consentir el tratamiento de tales datos en el momento de ser recabados.

2. Los datos de carácter personal que se refieran a la salud, violencia de género, vida sexual u origen racial de las personas solo serán recabados y tratados cuando por razones de interés público así lo establezca una ley o el interesado consienta expresamente.

3. Por lo que respecta a los datos de carácter personal relativos a la salud, se respetará lo dispuesto especialmente en la normativa de Seguridad Social, de prevención de riesgos laborales, fiscal o la universitaria.

4. Los datos relativos a discapacidad, concurrencia de incapacidad laboral, aptitud para el desempeño de un determinado puesto de trabajo o causa que justifica una determinada baja laboral, han de ser considerados datos relacionados con la salud de dichos afectados.

5. Los profesionales de la Universidad de Granada que desarrollen actividades directamente relacionadas con la salud de los trabajadores, estudiantes u otros pacientes, podrán tratar los datos de carácter personal relativos a la salud de las personas que a ellos acudan, de acuerdo con lo dispuesto en la normativa vigente en materia de sanidad, protección de la salud y prevención de riesgos laborales.

CAPÍTULO CUARTO

Usos y finalidades del tratamiento

Artículo 10. Calidad en el uso de los datos.

1. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades distintas para las que los datos fueron recogidos.

No se considerará incompatible el tratamiento posterior de los datos para fines históricos, estadísticos o científicos, sin perjuicio de que el interesado haya de ser convenientemente informado. La determinación de estos fines se ajustará a la legislación aplicable en la materia, ya sea estatal o autonómica, no pudiendo decidirse discrecionalmente dicho fin.

2. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del interesado. Se consideran exactos los datos facilitados directamente por el interesado.

3. Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

Artículo 11. Acceso a datos por cuenta de terceros.

1. El acceso por parte de un tercero a datos que consten en ficheros o tratamientos de los que sea responsable la Universidad de Granada, se realizará en condición de encargado del tratamiento cuando resulte necesario para la prestación de un servicio delimitado por la existencia de una relación jurídica que le vincula a la Universidad. En este caso, el acceso no será considerado cesión o comunicación de datos de carácter personal, no requiriendo por tanto el consentimiento del interesado, siempre que el acceso no tenga por finalidad el establecimiento de un nuevo vínculo entre quien accede a los datos y el interesado.

2. Solo se establecerá dicha relación con encargados del tratamiento que reúnan las garantías suficientes para considerar que cumplen con la normativa de protección de datos, para lo que se verificará su situación en el Registro General de Protección de Datos o se solicitará documentación relativa a los procedimientos establecidos para el tratamiento de datos de carácter personal.

3. La relación con todo encargado del tratamiento deberá formalizarse por escrito, ya sea remunerada o no, temporal o indefinida, y deberá respetar las exigencias establecidas por la LOPD y su Reglamento de desarrollo. Para ello, se adaptarán los Pliegos de Cláusulas Administrativas Particulares de la Universidad y los contratos de prestación de servicios de los que se deriven el tratamiento de datos de carácter personal, cuando no sean de aplicación los mencionados pliegos, utilizándose los modelos que procedan de los establecidos en el Anexo IV.

4. La copia de los pliegos o, en su caso, de los contratos y los acuerdos de confidencialidad suscritos con encargados del tratamiento deberá ser enviada a la Secretaría General para su reflejo en el Documento de Seguridad.

CAPÍTULO QUINTO

Régimen de cesión de datos de carácter personal

Artículo 12. Consentimiento para la cesión.

1. Los datos objeto de tratamiento solo podrán ser cedidos para el cumplimiento de fines directamente relacionados con la actividad legítima del cedente y del cesionario, lo que requerirá el consentimiento inequívoco del interesado.

2. No será preciso el consentimiento para la cesión o comunicación de datos cuando:

a) Una norma con rango de Ley o una norma de Derecho comunitario lo autorice, bien porque la cesión tenga por objeto satisfacer un interés legítimo de la Universidad amparado en dicha norma cuando no prevalezca el interés o los derechos y libertades de los interesados, o bien porque sea necesaria para que la Universidad cumpla un deber que le impone dicha norma.

b) Se trate de datos recogidos de fuentes accesibles al público y su destinatario sean otras Administraciones públicas. En otro caso, aun procediendo los datos de fuentes accesibles al público, la cesión deberá estar prevista por una ley para no requerir el consentimiento del interesado.

c) El tratamiento responda a la libre y legítima aceptación de una relación jurídica, cuyo desarrollo, cumplimiento y control comporte la comunicación de datos, siempre que se limite a la finalidad que la justifique.

d) La comunicación tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal, los Jueces o Tribunales, el Tribunal de Cuentas o las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas, y se realice en el ámbito de las funciones que la ley les atribuya expresamente.

e) La Universidad obtenga o elabore datos con destino a otra Administración Pública.

f) Se realice con destino a otra Administración Pública y tenga como objeto el tratamiento de los datos con fines históricos, científicos o estadísticos.

g) Se realice con destino a otra Administración Pública para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

3. Cuando no sea necesario el consentimiento para la cesión, el interesado en todo caso deberá ser informado de ella. Tanto para la información al interesado sobre la cesión de sus datos, como para la solicitud de su consentimiento, se emplearán los modelos recogidos en los Anexos II y III de este Reglamento, respectivamente, procediendo al cumplimiento de las obligaciones relativas a la cesión de datos en el mismo momento de la recogida de datos, de forma que no sea necesario dirigirse nuevamente al interesado.

4. Cuando la cesión se realice previo procedimiento de disociación de datos, no será aplicable la normativa de Protección de Datos de Carácter Personal.

Artículo 13. Datos especialmente protegidos.

1. La cesión de datos relativos a ideología, religión, creencias y afiliación sindical, requiere consentimiento expreso y por escrito del interesado, debiendo ser advertido de su derecho a no consentir la cesión de tales datos en el momento de ser recabados.

2. Los datos de carácter personal que se refieran a la salud, violencia de género, vida sexual u origen racial de las personas solo serán cedidos cuando por razones de interés público así lo establezca una ley o el interesado consienta expresamente.

3. Los datos de salud de los interesados podrán ser cedidos cuando sea necesario para solucionar una urgencia médico-sanitaria que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación estatal o autonómica sobre la materia.

Artículo 14. Obtención del consentimiento.

1. Para que el consentimiento sea válido a efectos de cesión de datos, el interesado debe conocer de forma inequívoca, al menos, lo siguiente:

- a) Tipo de datos objeto de la cesión.
- b) Finalidad a la que se destinarán los datos de la cesión.
- c) Actividades de las entidades cesionarias.

La obtención del consentimiento para su cesión podrá ser recabada por medios electrónicos que garanticen la identificación del interesado. A tal efecto, se incluyen entre ellos el correo electrónico corporativo para el personal y estudiantado de la Universidad de Granada y cualquier correo electrónico que el interesado hubiese indicado como medio de comunicación o notificación en el procedimiento administrativo de referencia.

2. El consentimiento para la cesión de datos tendrá carácter revocable en los mismos términos establecidos en el artículo 9 de este Reglamento. En caso de producirse, deberá comunicarse la revocación a las entidades cesionarias en el plazo de 10 días desde que se recibió la solicitud, instándoles a que cesen en el tratamiento de los datos del interesado.

Artículo 15. Procedimiento de cesión de datos.

1. La información relativa a miembros de la comunidad universitaria y a otras personas físicas solo se facilitará a externos cuando esté aprobada su cesión por la Secretaría General, pudiendo solicitarse informe a los Servicios Jurídicos de la Universidad cuando así se estime necesario.

2. Cuando el tratamiento sea realizado dentro del ámbito de la Universidad no se considerará que se está produciendo una cesión de datos, salvo que la finalidad para la que se utilicen los datos por la Unidad o Servicio que lo solicita sea distinta a aquella para la que se recogieron, sin perjuicio de que el interesado haya sido informado adecuadamente de las finalidades para las que sus datos fueron recabados y, en su caso, se haya solicitado su consentimiento.

3. Aquellas cesiones que tengan un carácter periódico solo serán revisadas para su valoración una vez. La Secretaría General podrá poner a disposición pública las cesiones que pueden ser realizadas sin necesidad de autorización.

4. Sin perjuicio del procedimiento de cesión establecido en los apartados anteriores, cualquier cesión de datos efectuada a un país que no sea miembro del Espacio Económico Europeo o sobre el que no se haya declarado un nivel adecuado de protección por la Agencia Española de Protección de Datos o la Comisión Europea, requerirá la previa supervisión del correspondiente Coordinador LOPD y el posterior pronunciamiento de la Secretaría General de la Universidad de Granada.

5. Para instar la cesión, el solicitante deberá utilizar el «formulario de solicitud de cesión de datos de carácter personal» que estará a disposición de los solicitantes en la página web de la Secretaría General y en la sede electrónica de la Universidad de Granada, en el que se compromete a un tratamiento de los datos recibidos acorde a la finalidad para la que han sido solicitados y a la normativa de Protección de Datos de Carácter Personal.

6. En caso de apreciarse la oportunidad de la cesión, la Secretaría General informará al Coordinador LOPD correspondiente de las finalidades para las que se solicitan los datos y del destinatario de la información si éste es externo, para que pueda verificar que el solicitante ha sido informado de las finalidades y en su caso de los cesionarios de sus datos de carácter personal y que se ha solicitado su consentimiento en el momento de la recogida de los datos, cuando dicha obligación no recaiga sobre el solicitante.

Una vez que el Coordinador LOPD envíe a Secretaría General el listado o fichero correspondiente, con las condiciones de seguridad necesarias, ésta se los remitirá al solicitante.

7. En el caso en que la solicitud sea desestimada, la Secretaría General se lo comunicará motivadamente al solicitante.

8. La Secretaría General mantendrá un archivo de los formularios de solicitud debidamente firmados, así como constancia del envío y copia de la información remitida.

9. Cualquier cesión de datos que no cumpla con este procedimiento será responsabilidad exclusiva de quien lo lleve a cabo, frente a terceros y frente a la propia Universidad de Granada.

Artículo 16. Cesiones de datos a autoridades judiciales y administrativas especiales.

1. La información sobre datos de carácter personal obrantes en ficheros de la Universidad de Granada que puede afectar a estudiantes, personal o terceros, será comunicada a autoridades judiciales y administrativas con sujeción al procedimiento legalmente establecido y a las reglas que se exponen a continuación. No se atenderán peticiones de información sobre datos de carácter personal no motivadas.

2. La cesión de datos a órganos judiciales y administrativos especiales será supervisada por el correspondiente Coordinador LOPD y, en cualquier caso, requerirá autorización expresa emitida desde la Secretaría General.

En los siguientes casos, procederá la autorización por parte de la Secretaría General de la Universidad de Granada, cuando además de lo contemplado en los puntos anteriores y en la normativa vigente al respecto, concorra alguna de las siguientes circunstancias:

a) Informaciones solicitadas por organismos judiciales: Se facilitarán los datos cuando estos sean solicitados mediando la intervención de la autoridad judicial.

b) Informaciones solicitadas por órganos gubernativos directamente relacionados con actuaciones preparatorias o complementarias de procesos judiciales: Serán facilitadas cuando conste claramente la intervención de órgano judicial concreto.

c) Informaciones solicitadas por los Cuerpos y Fuerzas de Seguridad del Estado: Se atenderá la solicitud cuando medie resolución judicial para la cesión de datos. No será necesario que medie orden judicial en los siguientes casos:

- En aquellas solicitudes concretas y específicas que se refieran a la existencia de un peligro real y grave para la seguridad pública o para la represión de infracciones penales.

- Cuando se trate de datos especialmente protegidos y sean absolutamente necesarios para los fines de una investigación concreta.

d) Otros organismos administrativos. Se facilitarán los datos cuando:

- La solicitud haya sido presentada por la Inspección Tributaria, la Agencia Estatal de Administración Tributaria o las Oficinas Recaudatorias de las Haciendas Locales, en virtud de lo establecido en los artículos 111 y 112 de la Ley General Tributaria, y el artículo 37 del Reglamento General de Inspección de Tributos o normativa vigente en cada momento, y siempre que la información solicitada tenga trascendencia tributaria.

- La solicitud sea presentada por el Instituto Nacional de la Seguridad Social o cualquiera de sus centros u oficinas, en el ejercicio de las competencias que le son propias.

- La solicitud sea presentada por la autoridad laboral correspondiente en el uso de las competencias que le son propias.

- La solicitud de datos se presente basada en la Ley 12/1989, de 12 de mayo, sobre Función Pública Estadística, para la elaboración de estudios de este carácter.

- La cesión sea obligatoria en virtud de una Ley.

CAPÍTULO SEXTO

Fin del tratamiento

Artículo 17. Calidad de los datos en la cancelación.

1. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

2. La cancelación dará lugar al bloqueo de los datos quedando fuera de los circuitos de explotación habituales y estableciéndose su custodia mediante un sistema que permita el control y registro de los accesos que se produzcan, con la finalidad de su puesta a disposición de las Administraciones públicas, los juzgados y los tribunales para atender a las posibles responsabilidades nacidas del tratamiento.

3. Podrán conservarse debidamente bloqueados durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

4. Una vez cumplido el período al que se refieren los párrafos anteriores, los datos solo podrán ser conservados previamente disociados.

CAPÍTULO SÉPTIMO

Derechos de los interesados

Artículo 18. Requisitos Generales.

1. La Secretaría General es el órgano de la Universidad de Granada encargado de atender, gestionar y tramitar el ejercicio de los derechos de los interesados, conforme a lo establecido en el presente Reglamento y en los procedimientos elaborados al efecto.

Excepcionalmente, el Defensor Universitario atenderá las solicitudes que se refieran a la documentación que sobre los interesados obre en su poder, en atención a los principios de reserva y confidencialidad que rigen su actuación, de acuerdo con lo establecido en el «Reglamento de organización y funcionamiento del Defensor Universitario de la Universidad de Granada».

2. A la hora de atender el ejercicio de los derechos de los interesados, se tendrán en cuenta los siguientes aspectos generales:

a) Los derechos de acceso, rectificación, cancelación y oposición (en adelante derechos ARCO) son personalísimos y serán ejercidos por el interesado frente a la Universidad de Granada, por lo que será necesario que el interesado acredite su identidad frente a ésta.

b) En el caso de que el interesado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de sus derechos podrá actuar su representante legal acreditando tal condición.

c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. Podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.

d) Estos derechos se configuran como independientes, de forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

e) No se exigirá contraprestación alguna por el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3. Los derechos de acceso, rectificación, cancelación y oposición se ejercerán mediante escrito dirigido a la Secretaría General y a través del Registro General de la Universidad y sus registros auxiliares, o por cualquiera de los medios previstos en la legislación vigente.

4. El escrito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición deberá realizarse en modelo normalizado, que estará disponible en la web corporativa de la Secretaría General y en la sede electrónica de la Universidad de Granada, teniendo en cuenta las siguientes consideraciones:

a) Cuando la solicitud se realice en papel, el interesado, a efectos de identificación, deberá acompañarla de una fotocopia de su documento nacional de identidad, pasaporte o tarjeta de residencia. En el caso de miembros de la comunidad universitaria, también se admitirá como válida la fotocopia del carné universitario inteligente.

b) En caso de representación, se deberá adjuntar a la solicitud el documento acreditativo de su otorgamiento y de la persona que lo representa.

c) Cuando proceda, se aportarán los documentos acreditativos de la petición que formula.

d) En el caso de que el ejercicio del derecho se refiera a un tratamiento de videovigilancia, se aportará una imagen actualizada del afectado, y se indicará la fecha y hora a que se refiere la captación.

La solicitud de rectificación deberá indicar el dato que es erróneo y la corrección que debe realizarse y deberá ir acompañada de la documentación justificativa de la rectificación solicitada, todo ello de forma que, en ningún caso, se pueda incurrir en posibles errores de interpretación.

En el caso de que la solicitud no cumpla dichos requisitos, se podrá solicitar subsanación al interesado para que la complete, concediéndole un plazo de diez días, transcurridos los cuales sin haber recibido contestación, se dará por desistido del ejercicio de su derecho.

5. Las solicitudes que no se realicen en los modelos normalizados disponibles serán objeto de requerimiento para su subsanación, y de no hacerlo en plazo serán inadmitidas por no ajustarse a lo establecido en el apartado 4 de este artículo. Esta inadmisión causará efecto, sin perjuicio de que el interesado pueda presentar nueva solicitud utilizando los cauces establecidos en el mencionado apartado.

6. La solicitud será contestada por escrito con independencia de que figuren o no datos personales del interesado en los ficheros en los plazos que se indican en los artículos siguientes, mediante comunicación notificada. En el caso de que la Universidad no disponga de datos del afectado, le será comunicada dicha circunstancia. Transcurridos los plazos establecidos sin haber contestado de forma expresa, el interesado podrá interponer una reclamación ante la Agencia Española de Protección de Datos.

7. Si el interesado solicita otro medio para hacer efectivo su derecho, se valorará si es posible atender su solicitud sin perjudicar derechos de terceros y sin que perturbe el normal funcionamiento de los servicios prestados por la Universidad de Granada.

Artículo 19. Derecho de acceso.

1. El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de éstos.

La información que la Universidad de Granada proporcione al interesado, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible y comprenderá todos los datos base del interesado que sean accesibles y los resultantes de cualquier elaboración o proceso informático.

2. En virtud del derecho de acceso, el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento. En ningún caso el ejercicio del derecho de acceso podrá suponer el acceso a datos de carácter personal de terceras personas.

No obstante, cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos.

3. El plazo de contestación a la solicitud de acceso será de un mes a contar desde su recepción o, en su caso, desde la recepción de la subsanación. La Universidad de Granada hará efectivo el derecho en el mismo momento de proceder a la contestación.

4. El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la legislación sobre procedimiento administrativo.

Artículo 20. Derechos de rectificación y cancelación.

1. El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

2. El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este Reglamento.

3. Los derechos de rectificación y cancelación se resolverán dentro de los diez días siguientes al de la recepción de su solicitud, lo que deberá ser notificado al interesado en dicho plazo.

Igualmente, si los datos rectificadas o cancelados hubieran sido cedidos previamente, la Secretaria General, con informe del correspondiente Coordinador LOPD, comunicará al cesionario la rectificación o cancelación efectuada, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar o cancelar los datos. La rectificación efectuada por el cesionario no requerirá comunicación al afectado.

4. En los casos en que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el Coordinador LOPD procederá a dictar las órdenes oportunas a fin de que se proceda al bloqueo de los datos con el fin de impedir su ulterior proceso o utilización.

Artículo 21. Derecho de oposición.

1. El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en él cuando:

a) No sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b) Se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial.

c) El tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, salvo que esté autorizado por una norma con rango de ley que establezca medidas que garanticen el interés legítimo del interesado, o se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estime pertinente, a fin de defender su derecho o interés.

2. El derecho de oposición se resolverán dentro de los diez días siguientes al de la recepción de su solicitud, lo que deberá ser notificado al interesado en dicho plazo.

Artículo 22. Denegación de los derechos.

Únicamente procederá la denegación de sus derechos al interesado cuando:

a) La solicitud no es realizada por el propio interesado o persona que le represente.

b) Así lo prevea una Ley o una norma de Derecho comunitario de aplicación directa.

c) Una Ley o norma de Derecho comunitario de aplicación directa impida al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

d) Se ejercite el derecho de acceso en intervalos inferiores a 12 meses, salvo que el interesado pueda acreditar un interés legítimo para hacerlo en un plazo inferior.

e) La imagen aportada por el interesado no coincida o existan dudas sobre su coincidencia con las imágenes captadas por el sistema de videovigilancia.

f) Se trate de datos que reflejen hechos constatados en un procedimiento administrativo, siempre que coincidan con éste y el interesado solicite su rectificación.

g) Los datos no puedan ser eliminados, debiendo conservarse durante plazos previstos en disposiciones que sean aplicables o en la relación contractual establecida con el interesado.

h) La cancelación pudiese causar un perjuicio a intereses legítimos del interesado o de terceros.

i) No se aleguen motivos fundados y legítimos para oponerse al tratamiento cuando no haya sido necesario el consentimiento del interesado.

j) No se cumpla cualquier otro requisito establecido en la normativa vigente sobre protección de datos de carácter personal o en este Reglamento.

En todo caso, en la comunicación que se realice se informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de la autoridad de control autonómica, sin perjuicio de que pueda interponer recurso en vía administrativa.

Artículo 23. Procedimiento interno de tramitación.

1. Recibida la solicitud por la Secretaría General, ésta valorará el cumplimiento de los requisitos generales de capacidad del interesado y de la solicitud y requerirá, en su caso, su subsanación.

Si la solicitud fuese recibida en otro Servicio o Unidad de la Universidad, deberá ser remitida, a la mayor brevedad posible, a la Secretaría General.

2. Si la solicitud reuniese los requisitos formales indicados, se procederá por parte de la Secretaría General a recabar los informes correspondientes, tanto del Coordinador LOPD como, en su caso, del técnico designado por el Centro de Servicios de Informática y Redes de Comunicaciones (CSIRC) si el tratamiento fuese automatizado o mixto.

3. Recibidos los informes en los plazos que en cada caso les serán indicados en la petición, la Secretaría General procederá a resolver y realizará la correspondiente comunicación al interesado dentro del plazo establecido.

En cualquier caso, deberá quedar constancia en la Secretaría General de todo el expediente en cuestión, así como de cuantos informes se hayan realizado para dar cumplimiento o no a lo solicitado.

CAPÍTULO OCTAVO

Videovigilancia

Artículo 24. Ámbito objetivo.

1. El tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquellas.

2. A los efectos del apartado anterior, se considerará:

a) Identificable una persona cuando su identidad pueda determinarse sin que ello requiera plazos o actividades desproporcionados.

b) Un dato de carácter personal, las imágenes y la información gráfica o fotográfica concerniente a personas físicas identificadas o identificables.

3. No se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.

4. Las referencias contenidas en este Reglamento a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en el apartado 1 del presente artículo.

Artículo 25. Principios de calidad, proporcionalidad y finalidad del tratamiento.

1. La instalación y mantenimiento de sistemas de videovigilancia en los recintos cuya responsabilidad corresponda a la Universidad de Granada deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia y las instrucciones que sobre ella dicte la Agencia Española de Protección de Datos o, en su caso, por el organismo de la Comunidad Autónoma que asuma las competencias en materia de protección de datos.

2. La instalación de cámaras o videocámaras solo será admisible cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

3. En cumplimiento del principio de proporcionalidad respecto al fin perseguido, las imágenes solo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

4. Las cámaras y videocámaras instaladas no podrán obtener imágenes de la vía pública, salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

Artículo 26. Información.

Los responsables de las instalaciones que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de la LOPD. A tal efecto, dispondrán las siguientes medidas:

a) Colocar el distintivo informativo, que debe estar ubicado en un lugar suficientemente visible, tanto en espacios abiertos como cerrados. Salvo que la actividad del espacio requiera o aconseje una mayor información, se considera suficiente que haya un distintivo informativo en cada una de las puertas exteriores de acceso a los edificios o recintos. El contenido y el diseño del distintivo informativo será el establecido por Secretaría General.

b) Tener a disposición de los interesados impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999. A tal efecto, el modelo de impreso estará disponible, al menos, en las conserjerías de los edificios y, en cualquier caso, se podrá descargar desde la web corporativa de Secretaría General. El modelo de impreso será aprobado por Secretaría General.

Artículo 27. Derechos de acceso, rectificación, cancelación y oposición.

En el ejercicio de los derechos de acceso, rectificación, cancelación y oposición se actuará según lo previsto en el artículo 18.4 de este Reglamento.

Artículo 28. Cancelación de los datos.

1. Las imágenes obtenidas mediante sistemas de videovigilancia serán canceladas en el plazo máximo de un mes desde su captación.

2. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo, deberá procederse a la supresión.

Artículo 29. Seguridad y confidencialidad.

1. La Gerencia deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de las imágenes y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

2. El acceso a todos los equipos de grabación de imágenes de videovigilancia instalados en la Universidad de Granada se hará exclusivamente a través del Departamento de Seguridad. A tal efecto, los responsables de las distintas instalaciones dispondrán de un plazo de tres meses a partir de la entrada en vigor de este Reglamento para adoptar las medidas necesarias.

3. El mantenimiento del servidor central de videovigilancia corresponde al Centro de Servicios de Informática y Telecomunicaciones, sin perjuicio de que el Departamento de Seguridad tenga acceso para realizar las tareas de su competencia relativas a grabación, captación, transmisión, conservación, y almacenamiento de imágenes.

4. Asimismo, cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las imágenes, deberá de observar la debida reserva, confidencialidad y sigilo.

CAPÍTULO NOVENO

Funciones y obligaciones de las figuras responsables

Artículo 30. Responsable del fichero.

1. El Responsable del fichero será quien solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

2. A los efectos del presente Reglamento, el Responsable del fichero será la Universidad de Granada, aunque sus funciones serán asumidas por la Secretaría General, los Responsables de Seguridad y los Coordinadores LOPD, sin perjuicio de que cada órgano administrativo, en atención a sus competencias, asumirá la responsabilidad sobre las finalidades, contenido y uso de los datos que trate.

Artículo 31. Designación de Responsables.

1. El nombramiento de los Coordinadores LOPD corresponderá al Rector, a propuesta del Gerente, oídos los responsables de área, servicio, unidad u órgano equivalente, excepto cuando las obligaciones recaigan en un órgano concreto o sobre determinados puestos de trabajo que conlleven dicha responsabilidad.

2. El Rector podrá nombrar, a propuesta del Secretario General, uno o varios responsables de seguridad en función de las específicas características de determinados ficheros. La designación de éstos no exonerará de responsabilidad al Responsable del fichero.

Artículo 32. Funciones y obligaciones de la Secretaría General.

a) Velar por el cumplimiento de la normativa de protección de datos de carácter personal en la Universidad y coordinar las actuaciones en esta materia.

b) Elaborar y mantener actualizado el Documento de Seguridad, con la colaboración de los Coordinadores LOPD.

c) Notificar a la Agencia Española de Protección de Datos la creación, modificación o supresión de los ficheros de datos de carácter personal, una vez valoradas las indicaciones de los correspondientes Coordinadores LOPD.

d) Atender el ejercicio de los derechos ARCO de los interesados de acuerdo con el procedimiento establecido en el Documento de Seguridad, para lo que solicitará a los correspondientes Coordinadores LOPD la información necesaria en relación con el tratamiento efectivamente realizado.

e) Resolver las solicitudes de ejercicio de los derechos ARCO de los interesados.

f) Informar a los correspondientes Coordinadores LOPD el sentido de la resolución sobre el ejercicio de los derechos de los interesados, para que éstos puedan excluir o rectificar los datos afectados o, en su caso, facilitar su acceso por el interesado.

g) Autorizar cualquier cesión de datos a terceros, pudiendo consistir en autorizaciones genéricas cuando los envíos fuesen periódicos y respondan a una misma finalidad y destinatario.

h) Resolver en el caso de que existan discrepancias entre servicios o unidades en cuanto a las responsabilidades en la gestión relacionada con el tratamiento de datos de carácter personal.

i) Atender los requerimientos de la Agencia Española de Protección de Datos.

Artículo 33. Funciones y obligaciones del Responsable de Seguridad.

Los Responsables de Seguridad tendrán las siguientes funciones y obligaciones en su ámbito competencial:

a) Coordinar y controlar las medidas de seguridad definidas en el Documento de Seguridad.

b) Analizar los informes de auditoría y elevar a la Secretaría General las conclusiones del análisis del informe de auditoría.

c) Supervisar los mecanismos que permiten el control de accesos.

d) Revisar periódicamente la información de control registrada.

e) Elaborar mensualmente un informe de las revisiones efectuadas y los problemas detectados.

f) Guardar secreto de los datos de carácter personal que pueda conocer, así como sobre controles y posibles vulnerabilidades, incluso después de haber causado baja o traslado de la Universidad.

Artículo 34. Funciones y obligaciones del Coordinador LOPD.

1. Las funciones y obligaciones establecidas en este artículo afectarán a cada Coordinador LOPD en función del área, servicio, unidad o equivalente, bajo su responsabilidad. Cuando el tratamiento sea muy amplio y comprenda diversos ficheros, podrán nombrarse varios Coordinadores LOPD en cada área, servicio, unidad o equivalente.

2. Las funciones y obligaciones del Coordinador LOPD, sin perjuicio de cualesquiera otras que se establezcan en este Reglamento, son las siguientes:

a) Determinar quién puede acceder a los datos de carácter personal y siempre que sean necesarios para la función que realice.

b) Guardar secreto de la información de carácter personal que conozca en el desempeño de su función, aun después de haber abandonado la Universidad de Granada.

c) Supervisar la realización de nuevos formularios de recogida de datos de carácter personal relativos al tratamiento correspondiente, de forma que, de no haber sido el interesado informado con anterioridad, lleven incorporada la leyenda informativa.

d) Informar a la Secretaría General de la necesidad de creación de nuevos ficheros, o de la modificación o supresión de los ya existentes.

e) Informar, con carácter previo, al CSIRC de la creación de nuevos ficheros, para que, desde el punto de vista técnico, se consideren la plataforma y ubicación más idóneas y los controles necesarios para la protección de los contenidos.

f) Conservar, en la medida de lo posible, en archivadores o armarios, en ambos casos con cerradura, los datos contenidos en ficheros en papel o parcialmente automatizados.

g) Comunicar a la Secretaría General la necesidad de realizar nuevas cesiones de datos de carácter personal para que las evalúe y determine si es necesario el consentimiento del interesado.

h) Comunicar a la Secretaría General, para que pueda evaluar su legalidad, los supuestos no previstos en la Ley en los que se recaben datos de carácter personal de personas distintas del interesado (tales como compras o adquisición de bases de datos).

i) Supervisar el tratamiento de datos especialmente protegidos llevado a cabo por el personal de su área, cuando dicho tratamiento no sea habitual.

j) Autorizar el envío de correos electrónicos cuando contengan datos de carácter personal, pudiendo consistir en autorizaciones genéricas cuando los envíos fuesen periódicos y respondan a una misma finalidad y destinatario. Cuando dicho envío conlleve la cesión de datos, se remitirá a Secretaría General para su resolución.

k) Autorizar la grabación de soportes informáticos que contengan datos de carácter personal, en tanto dicha función no sea centralizada por el CSIRC.

l) Autorizar la salida de la Universidad de soportes informáticos o documentos que contengan datos de carácter personal, pudiendo consistir en autorizaciones genéricas cuando los envíos fuesen periódicos y respondan a una misma finalidad y destinatario. Cuando dicha salida conlleve la cesión de datos, se remitirá a Secretaría General para su resolución.

m) Comunicar a la Secretaría General cualquier tratamiento de datos de carácter personal por parte de terceros que presten algún servicio a la Universidad, y trasladar copia de los pliegos o, en su caso, del contrato o del acuerdo de confidencialidad para su reflejo en el Documento de Seguridad.

n) Atender cualquier solicitud por parte de Secretaría General relacionada con el ejercicio de derechos de acceso, rectificación, cancelación u oposición por parte de los interesados, en los plazos que se le indiquen. En caso de recibir directamente una solicitud, se la remitirá a Secretaría General, a efectos de que ésta pueda ser contestada con el contenido legalmente establecido.

o) Elaborar relaciones de personal con acceso a los lugares donde se almacenen los expedientes o los documentos que contengan datos de carácter personal, que podrán ser requeridos en caso de inspección o auditoría.

p) Mantener los registros y relaciones anteriores a disposición de auditorías o inspecciones en materia de protección de datos.

q) Gestionar las incidencias que se refieran a los datos no automatizados que forman parte del tratamiento realizado en su área, notificando su resolución mediante los sistemas establecidos por la Universidad.

Artículo 35. Funciones y obligaciones de los usuarios.

Las funciones y obligaciones de los usuarios, definidos en la letra aa) del Anexo I, son las siguientes:

a) Acceder únicamente a los datos de carácter personal a los que esté autorizado, necesarios para la función que realice.

b) Guardar secreto de la información de carácter personal que conozca en el desempeño de su función aun después de haber abandonado la Universidad.

c) Conocer la normativa interna en materia de seguridad y especialmente la referente a protección de datos de carácter personal, así como las consecuencias de su incumplimiento.

d) Respetar los mecanismos y dispositivos de seguridad, evitando cualquier intento de acceso no autorizado a datos o recursos; informar de posibles debilidades en los controles y no poner en peligro la disponibilidad de los datos, ni su confidencialidad o integridad.

e) Usar de forma adecuada los mecanismos de identificación y autenticación ante los sistemas de información, ya sean contraseñas o sistemas más avanzados, y en ambos casos, mediante acceso local o a través de redes de comunicaciones, cuando esté así previsto. En el caso de contraseñas, cumplir lo establecido en la normativa, especialmente en cuanto a su asignación, composición de caracteres, distribución, custodia y almacenamiento, así como al cambio con la periodicidad que se determine.

f) No utilizar el correo electrónico u otros medios de comunicación interna o con el exterior para transmitir mensajes que contengan o lleven adjuntos datos de carácter personal que por sus características, volumen o destinatarios puedan poner en peligro la confidencialidad o la integridad de los datos. En caso necesario, deberá estar debidamente autorizado en el Documento de Seguridad.

g) Comunicar al correspondiente Responsable de Seguridad cualquier incidencia de la que tenga conocimiento en materia de seguridad, que pueda afectar a datos de carácter personal.

h) Conocer el procedimiento a seguir en el ejercicio de derechos ARCO para informar a los solicitantes y, en su caso, remitir las solicitudes a Secretaría General.

i) No realizar transferencias de ficheros con datos de carácter personal entre sistemas o descargas en equipos, salvo en los casos expresamente autorizados y protegiendo después los contenidos para evitar difusión o copias no autorizadas.

j) Dirigir a impresoras protegidas los listados que contengan datos de carácter personal que requieran protección y recogerlos con celeridad para evitar su difusión, copia o sustracción.

k) No sacar equipos o soportes de las instalaciones sin la autorización necesaria, y en todo caso, con los controles que se hayan establecido.

l) Proteger los datos personales de la Universidad que excepcionalmente tuvieran que almacenarse o usarse fuera del lugar de trabajo, ya sea en el propio domicilio o en otras instalaciones alternativas, tanto en sistemas fijos como en portátiles.

m) Salir de los ordenadores personales o terminales cuando vaya a estar ausente de su puesto durante un tiempo superior al fijado en los procedimientos para cada caso, de modo que el sistema le pida de nuevo que se identifique, con independencia de que el protector de pantalla se pueda activar automáticamente.

n) Evitar que la información que muestra la pantalla en su puesto de trabajo pueda ser visible por terceros ajenos a la Universidad o personas no autorizadas.

o) Entregar, cuando se le requiera por el CSIRC y, especialmente, cuando vaya a causar baja o traslado de la Universidad, las llaves, claves, tarjetas de identificación, material, documentación, equipos, contraseñas, y cuantos activos sean propiedad de la Universidad.

DISPOSICIONES ADICIONALES

Disposición adicional primera. Actuaciones ante la Agencia Española de Protección de Datos.

Corresponde al Secretario General, asesorado, en su caso, por el personal técnico que se determine, la interlocución y el mantenimiento de las relaciones institucionales con la Agencia Española de Protección de Datos y, en su caso, con el organismo de la Comunidad Autónoma que asuma las competencias en materia de protección de datos, sin perjuicio de la colaboración del Responsable de Seguridad y de los Coordinadores LOPD.

En el caso de que una unidad de la Universidad de Granada reciba aviso de inspección o solicitud de información de la Agencia Española de Protección de Datos u organismo de la Comunidad Autónoma, lo pondrá en conocimiento de la Secretaría General con la mayor celeridad posible. A continuación, se reunirá la correspondiente comisión de estudio en la que, como mínimo, deberá estar presente el personal técnico que se determine, el Coordinador afectado por la inspección y el Responsable de Seguridad a fin de estudiar el objeto de la inspección.

La Secretaría General remitirá el informe que proceda a la Agencia Española de Protección de Datos.

Disposición adicional segunda. Denominación de género.

Todas las denominaciones contenidas en este Reglamento referidas a órganos unipersonales de gobierno y representación, se entenderán realizadas y se utilizarán indistintamente en género masculino y femenino, según el sexo del titular que los desempeñe.

DISPOSICIÓN TRANSITORIA

Las áreas, servicios, unidades o equivalentes de la Universidad de Granada adoptarán las medidas oportunas para que, en el plazo máximo de seis meses desde la entrada en vigor del presente Reglamento, se dé cumplimiento a lo dispuesto en sus Anexos II y III.

DISPOSICIONES FINALES

Disposición final primera. Instrucciones de desarrollo.

Se faculta a la Secretaría General para dictar cuantas instrucciones sean necesarias para el desarrollo del presente Reglamento y para modificar el contenido de los modelos incluidos en los Anexos II, III y IV.

Disposición final segunda. Medidas técnicas de seguridad de carácter centralizado.

Sin perjuicio de lo establecido en este Reglamento, corresponde al Centro de Servicios de Informática y Redes de Comunicación (CSIRC) la implantación de las medidas técnicas de seguridad de carácter centralizado relativas a redes y sistemas informáticos que garanticen la protección de los datos de carácter personal.

Disposición final tercera. Entrada en vigor.

El presente Reglamento entrará en vigor el día siguiente de su publicación en el Boletín Oficial de la Universidad de Granada (BOUGR), sin perjuicio de su publicación en el Boletín Oficial de la Junta de Andalucía (BOJA).

ANEXO I

Definiciones

A los efectos previstos en este Reglamento se entenderá por:

- a) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.
- b) Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en su identificación y reserva con el fin de impedir su tratamiento, excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y solo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.
- c) Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado.
- d) Cesionario o destinatario de la cesión: Toda persona o entidad, de titularidad pública o privada, receptora de los datos cedidos.
- e) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
- f) Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.
- g) Datos de carácter personal relacionados con la salud: Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.
- h) Documento: Todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.
- i) Documento de Seguridad: Documento que recoge las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente, de obligado cumplimiento para el personal con acceso a los sistemas de información.
- j) Destinatario: La persona física o jurídica, pública o privada, u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
- k) Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con éste y delimita el ámbito de su actuación para la prestación de un servicio. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
- l) Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
- m) Ficheros de titularidad pública: Los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de ellas y las Corporaciones de Derecho público, siempre que su finalidad sea el ejercicio de potestades de Derecho público.
- n) Fichero no automatizado: Todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.
- o) Fuentes accesibles al público: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Se entenderá que solo tendrán el carácter de fuentes accesibles al público:
 - a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.
 - b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.
 - c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, capítulo, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.

d) Los diarios y boletines oficiales.

e) Los medios de comunicación social. La red de internet, en sí misma, no será considerada como un medio de comunicación social, sin perjuicio de que sea empleada como plataforma de difusión por dichos medios.

p) Persona identificable: Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

q) Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

r) Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

s) Responsable de Seguridad: Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

t) Sistemas de información: Conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

u) Sistema de tratamiento: Modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

v) Soporte: Objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

w) Tercero: La persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento. Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

x) Transferencia internacional de datos: Tratamiento de datos que supone una transmisión fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

y) Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en dichos documentos.

z) Tratamiento de datos: Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

aa) Usuario: Sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

ANEXO II

Cláusula informativa para la recogida y cesión de datos de carácter personal

1. Cuando se vaya a proceder a la recogida y cesión de datos de carácter personal, el formulario deberá incluir la siguiente cláusula informativa:

«Sus datos personales, aportados en la solicitud y contenidos en la documentación que, en su caso, la acompañe, serán tratados por la Universidad de Granada, con sede en Avda. del Hospicio, s/n, 18071, Granada, con la finalidad de Sus datos serán cedidos a..... con la finalidad de..... Puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición ante la Secretaría General de la Universidad de Granada, en la dirección anteriormente indicada, mediante solicitud escrita acompañada de copia del DNI. De todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.»

2. La presente leyenda debe incorporarse en todos los formularios de recogida de datos, salvo que el interesado ya haya sido previamente informado. Cualquier procedimiento mediante el cual se recaben datos por primera vez, debe incluir la leyenda informativa del punto anterior.

3. El interesado debe firmar el documento en el que se incluya esta leyenda informativa y debe quedar en poder de la Universidad de Granada.

ANEXO III

Formulario para recabar el consentimiento para la recogida y cesión de datos de carácter personal

1. Cuando sea necesario solicitar el consentimiento del interesado, la redacción será la siguiente:

«Autoriza que sus datos personales aportados en la solicitud y contenidos en la documentación que en su caso la acompañe serán tratados por la Universidad de Granada, con sede en Avda. del Hospicio, s/n, 18071, Granada, con la finalidad de (indicar las finalidades principales y accesorias del tratamiento) Si no consiente en el uso de sus datos con la finalidad de..... marque la siguiente casilla

Con la finalidad de..... autoriza que sus datos sean cedidos a..... (indicar destinatarios).

En caso de no autorizar la cesión, marque la siguiente casilla

Puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición ante la Secretaría General de la Universidad de Granada en la dirección anteriormente indicada mediante solicitud escrita acompañada de copia del DNI. De todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.»

2. Se recabará el consentimiento expreso del interesado mediante la inclusión de esta fórmula en los impresos en los que se recaben datos para tratamiento que no responda a alguna de las excepciones establecidas en el presente Reglamento. En el caso de formularios electrónicos se realizarán las adaptaciones necesarias para cumplir con la finalidad establecida.

3. En los casos en que no se den las garantías técnicas necesarias que permitan acreditar la efectiva prestación del consentimiento, éste no se recabará por vía telemática. En cualquier caso, se entenderá que cumplen con estas garantías procedimientos telemáticos que el interesado pueda iniciar con certificado digital o utilizando el usuario y contraseña asignados por el CSIRC con la finalidad de que los usuarios de la Universidad de Granada puedan acceder usando el «acceso identificado a servicios on-line de la Universidad de Granada».

4. El interesado debe firmar el documento en el que se incluya esta fórmula de autorización y éste quedará en poder de la Universidad.

ANEXO IV

Modelos de cláusula de protección de datos de carácter personal y medidas de seguridad y de acuerdo de confidencialidad para el tratamiento de datos de carácter personal y medidas de seguridad

1. Con el objeto de que se recojan las cláusulas correspondientes a protección de datos y medidas de seguridad en los Pliegos de Cláusulas Administrativas Particulares y, cuando los pliegos no sean aplicables, en todo contrato con un tercero que preste servicios a la Universidad y del que se derive el tratamiento de datos de carácter personal contenidos en ficheros titularidad de la Universidad, se contemplan en este Anexo los siguientes modelos:

A) Modelo de cláusula de protección de datos de carácter personal y medidas de seguridad, para incluir en los Pliegos de Cláusulas Administrativas Particulares y, cuando los pliegos no sean aplicables, en todo contrato que se vaya a suscribir con un tercero.

B) Modelo de acuerdo de confidencialidad para el tratamiento de datos de carácter personal y medidas de seguridad, para completar todo contrato ya suscrito con un tercero.

2. Se faculta a la Secretaría General para que adapte estos modelos cuando se trate de una prestación de servicios consistente solo en el acceso a datos de carácter personal.

A) Modelo de cláusula de protección de datos de carácter personal y medidas de seguridad.

(Para incorporar en los Pliegos de Cláusulas Administrativas Particulares y, cuando los pliegos no sean aplicables, en todo contrato de prestación de servicios que se celebre del que se derive el tratamiento de datos de carácter personal.)

1. Prestaciones y propiedad de los datos.

En el contexto de la prestación de servicios encargada por la Universidad y con la finalidad mencionada en el presente contrato, la Universidad proporciona a [denominación empresa] los datos de carácter personal relativos a [especificar tipo de datos] (en adelante los «datos»), con el fin de hacer posible la prestación de los servicios encomendados.

Para ello, y a los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, [denominación empresa] como prestataria del servicio de [especificar servicio prestado] se convierte en Encargado del Tratamiento, comprometiéndose al cumplimiento de las obligaciones que le son inherentes.

[denominación empresa] reconoce expresamente que los datos de los que es encargado del tratamiento son de exclusiva propiedad de la Universidad de Granada, por lo que no podrá aplicarlos o utilizarlos con fines distintos a los previstos en el contrato de prestación de servicios.

[denominación empresa] únicamente podrá tener acceso a aquellos datos que la Universidad de Granada le proporcione en cumplimiento del presente contrato, y procederá a su tratamiento de acuerdo con las instrucciones proporcionadas, no constituyendo, en ningún caso, dicho acceso una comunicación de datos, ni siquiera a efectos de su conservación.

2. Tratamiento de datos.

[denominación empresa] se compromete a tratar los datos con la finalidad exclusiva de la realización del servicio. Una vez realizada la prestación del servicio, [denominación empresa] se compromete a destruir los datos proporcionados por la Universidad así como el resultado de cualquier elaboración de los mismos y los soportes o documentos en que se halle recogida la información o, en su caso, a devolvérselos a la Universidad en función de la decisión tomada por la misma en cada caso.

En caso de ser necesario que [denominación empresa] conserve los datos o una parte de los mismos a efectos de la atención de posibles responsabilidades que pudiesen derivarse del tratamiento, estos deberán permanecer convenientemente bloqueados hasta que transcurran los plazos de prescripción correspondientes, momento en que deberán ser destruidos. La Universidad deberá tener conocimiento de ellos así como de las medidas que garanticen el adecuado bloqueo de los datos y finalmente su destrucción.

[denominación empresa] se obliga a utilizar los datos a los que le dé acceso la Universidad de Granada única y exclusivamente para los fines del presente contrato y a guardar secreto profesional respecto a todos los datos de carácter personal que conozca y a los que tenga acceso durante la realización del contrato de prestación de servicios. Igualmente, se obliga a custodiar e impedir el acceso a los datos de carácter personal a cualquier tercero ajeno al presente contrato. Las anteriores obligaciones se extienden a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta de [denominación empresa] y subsistirán aun después de terminados los tratamientos efectuados en el marco del presente contrato.

[denominación empresa] se compromete a comunicar y hacer cumplir a sus empleados, asignados al proyecto, las obligaciones establecidas en esta cláusula.

Cualquier uso de los datos que no se ajuste a lo dispuesto en la presente cláusula, será responsabilidad exclusiva de [denominación empresa] frente a terceros y frente a la Universidad ante la que responderá por los daños y perjuicios que le hubiere podido causar, siendo considerado también responsable del tratamiento a estos efectos.

3. Medidas de seguridad.

[denominación empresa] manifiesta cumplir con la normativa vigente en materia de protección de datos de carácter personal y, en particular, con las medidas de seguridad correspondientes a sus ficheros.

[denominación empresa] se compromete a aplicar a los datos facilitados por la Universidad de Granada, las medidas de seguridad de nivel [especificar el nivel de seguridad aplicable] previstas en el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, de acuerdo con las categorías de datos tratados. En todo caso las siguientes:

(En el caso en que durante la prestación del servicio se produzca el acceso y tratamiento de datos de nivel básico incluir el siguiente texto.)

a) En el caso en que el servicio sea prestado en los locales de [denominación empresa], ésta dispondrá de un documento de seguridad de obligado cumplimiento en el que se recogerán las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente.

b) El personal de [denominación empresa] conocerá sus deberes de custodia y confidencialidad respecto a los datos o la documentación que tengan a su cargo, sus funciones y obligaciones, así como las normas de seguridad que afectan al desarrollo de las mismas, encontrándose claramente definidas y documentadas.

c) En el caso en que el tratamiento se realice en los sistemas de [denominación empresa], ésta dispondrá de mecanismos para identificar y autenticar de forma inequívoca y personalizada a los usuarios del sistema, y si la autenticación está basada en contraseñas, éstas caducarán periódicamente y serán almacenadas de forma ininteligible.

d) El sistema tendrá establecidos perfiles de acceso que permitirán, en atención a la asignación de obligaciones y responsabilidades relacionadas con el tratamiento de datos de carácter personal, que cada usuario acceda únicamente a aquellos recursos que precise para el desarrollo de sus funciones. La asignación del perfil y otorgamiento del acceso se hará mediante un procedimiento documentado y auditable.

e) Si los sistemas empleados en el tratamiento fuesen propiedad de la Universidad de Granada, [denominación empresa] adoptará los mecanismos de control implantados por ésta, comprometiéndose el personal de la [denominación empresa] al cumplimiento de las medidas y procedimientos asociados al mismo.

f) [denominación empresa] mantendrá un registro de las incidencias, acorde a lo establecido en el artículo 90 del RDLOPD, que puedan afectar a la seguridad de los datos de carácter personal. [denominación empresa] comunicará a la Universidad de Granada un resumen de las incidencias acaecidas, con la periodicidad que se establezca.

g) Si los sistemas empleados en el tratamiento fuesen propiedad de la Universidad de Granada, el personal de [denominación empresa] utilizará el sistema de notificación de incidencias de la Universidad de Granada, y se preocupará de que su personal conozca su responsabilidad en la notificación, considerándose el conocimiento y la no notificación de una incidencia como una falta contra la seguridad.

h) [denominación empresa] dispondrá de procedimientos de copias diarias, y de recuperación que puedan garantizar la reconstrucción en el estado en que se encontraban los datos en caso de producirse su pérdida o destrucción. La correcta definición, funcionamiento y aplicación de dichos procedimientos se verificará cada seis meses, quedando registro de dichas verificaciones.

i) Si la prestación de servicios objeto del presente contrato conlleva la creación de soportes informáticos o en papel con datos de carácter personal, estarán sujetos a procedimientos de identificación, inventario y almacenamiento de acuerdo con criterios de archivo definidos y acceso restringido. Las salidas de dichos soportes y documentos estarán autorizadas de acuerdo con relaciones de responsables debidamente designados, disponiendo [denominación empresa] de mecanismos de destrucción de soportes y documentos, de forma que se evite su recuperación posterior.

j) En dicho caso el traslado de soportes y documentos que contengan datos de carácter personal, se realizará protegido de forma que se evite su sustracción, pérdida, manipulación o acceso indebido.

k) Si fuese necesario realizar una parte del tratamiento fuera de los locales de la [denominación empresa] incluso mediante el uso de dispositivos portátiles, dicha actuación será autorizada de acuerdo con relaciones de responsables debidamente designados.

l) Las transmisiones y accesos a través de redes de telecomunicaciones se realizarán con medidas que garanticen un nivel de seguridad equivalente a los accesos en modo local.

m) No se realizarán pruebas con datos reales procedentes de los ficheros titularidad de la Universidad de Granada salvo que ésta lo autorice expresamente, debiendo en ese caso respetar durante el proceso las medidas de seguridad acordes al nivel de seguridad que corresponda a las categorías de datos empleados. Dicho proceso se reflejará en un registro.

(En el caso en que durante la prestación del servicio se produzca el acceso y tratamiento de datos de nivel medio incluir además el siguiente texto.)

n) Los mecanismos de acceso a los sistemas donde se estén tratando datos de carácter personal por cuenta de la Universidad de Granada, impedirán intentar reiteradamente un acceso no autorizado.

o) Si la prestación de servicios objeto del presente contrato conlleva la creación de soportes informáticos o en papel con datos de carácter personal y fuese necesario su traslado, [denominación empresa] contará con sistemas de registro de entradas y salidas acordes a lo establecido en el artículo 97 del RDLOPD.

p) Los procedimientos de recuperación de datos requerirán autorización de la Universidad de Granada y quedarán debidamente registrados.

q) [denominación empresa] habrá designado al menos un responsable de seguridad encargado de coordinar y controlar las medidas de seguridad aplicables a los tratamientos de datos de carácter personal, sin perjuicio de la coordinación llevada a cabo por el responsable de seguridad designado por la Universidad de Granada para lo cual recibirá la información de control que periódicamente le deba ser facilitada por [denominación empresa].

r) [denominación empresa] contará con medidas de acceso físico que impidan a toda aquella persona que no esté convenientemente autorizada el acceso a los lugares donde se encuentran los equipos.

s) La Universidad de Granada podrá realizar auditorías de los sistemas de información [denominación empresa], donde se estén realizando los tratamientos de datos de carácter personal, con el fin de verificar el cumplimiento de las medidas recogidas en el presente Anexo, al menos cada dos años, siempre que se hagan de forma que no se altere el adecuado desarrollo de la prestación del servicio contratado.

(En el caso en que durante la prestación del servicio se produzca el acceso y tratamiento de datos de nivel alto incluir además el siguiente texto.)

t) Los sistemas de [denominación empresa] empleados para el tratamiento de datos de carácter personal, dispondrán de mecanismos de registro de cualquier acceso que se produzca a datos considerados especialmente protegidos por la LOPD y así como a cualquier tipo de dato al que se le asigne un nivel alto de medidas de seguridad. Dichos registros se conservarán al menos durante dos años. En caso de detectar incidencias en la información de control registrada [denominación empresa] se lo comunicará a la Universidad de Granada.

u) Si la prestación de servicios objeto del presente contrato conlleva la creación de soportes informáticos o en papel con datos de carácter personal, su método de etiquetado se realizará con sistemas de codificación debidamente custodiados que impidan identificar su contenido a terceros. Dichos soportes y documentos se almacenarán protegidos, en áreas de acceso restringido que quedará debidamente registrado.

v) En dicho caso, estará controlada la reproducción de información con datos de carácter personal y sometida a procesos de destrucción una vez finalizado su uso.

w) El traslado de datos de carácter personal fuera de las instalaciones de [denominación empresa] donde se esté realizando el tratamiento, en soportes informáticos o en ordenadores portátiles se realizará cifrando dichos datos o con un mecanismo que ofrezca garantías similares.

x) [denominación empresa] dispondrá al menos de dos juegos de copias de seguridad y procedimientos de recuperación de los datos de carácter personal, debiendo almacenarse uno de ellos debidamente protegido, en una ubicación protegida y suficientemente alejada del Centro de Proceso de Datos de forma que se garantice su recuperación en caso de tener lugar una incidencia importante.

y) La transmisión de datos de carácter personal a través de redes de comunicaciones públicas o inalámbricas se hará cifrado o mediante mecanismo similar.

El incumplimiento de este compromiso será responsabilidad exclusiva de [denominación empresa], que responderá frente a terceros y frente a la propia Universidad de los daños y perjuicios que pudieran generarse.

4. Subcesiones.

[denominación empresa] se compromete a no realizar ninguna cesión de los datos a los que accede. Ello, salvo que tal cesión fuese imprescindible para la efectiva prestación del servicio, en cuyo caso, [denominación empresa] solicitará la subcesión previa autorización de la Universidad, que podrá otorgarla o resolver el contrato de servicios con [denominación empresa].

5. Subcontratación.

Queda prohibida la subcontratación de todos o parte de los servicios contratados por la Universidad de Granada a [denominación empresa]. Si durante la prestación del servicio resultase necesario subcontratar todo o una parte del mismo dicha subcontratación deberá ser expresamente autorizada por la Universidad de Granada, obligándose [denominación empresa], a exigir contractualmente a el subcontratista, la implementación en sus instalaciones de las medidas de seguridad previstas en el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, así como los demás extremos previstos en los artículos 9, 10 y 12 de la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás concordantes del citado Real Decreto que la desarrolla reglamentariamente. Dicho contrato deberá contener expresa mención a las instrucciones dictadas por la Universidad de Granada en relación con la prestación del servicio, sin perjuicio de cualesquiera otras adicionales que [denominación empresa] exija al subcontratista en el marco de las establecidas por la Universidad de Granada. A estos efectos el subcontratista será considerado encargado del tratamiento.

(En caso de ser conocida previamente la necesidad de subcontratación dicha cláusula será sustituida por la siguiente):

La Universidad de Granada, autoriza expresamente y mediante la presente estipulación, a [denominación empresa], la cual acepta, a subcontratar los siguientes servicios:

Lo que supone el tratamiento de los datos contenidos en los ficheros denominados «[incluir el nombre de los ficheros accedidos]», a las entidades [denominación subcontratista 1] y/o [denominación subcontratista 2], obligándose [denominación empresa], a exigir contractualmente a éstas, la implementación en sus instalaciones de las medidas de seguridad previstas en el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, así como los demás extremos previstos en los artículos 9, 10 y 12 de la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás concordantes del citado Real Decreto que la desarrolla reglamentariamente. Dicho contrato deberá contener expresa mención a las instrucciones dictadas por la Universidad de Granada en relación con la prestación del servicio, sin perjuicio de cualesquiera otras adicionales que [denominación empresa] exija al/los subcontratista/s en el marco de las establecidas por la Universidad de Granada. A estos efectos el subcontratista será considerado encargado del tratamiento.

6. Ejercicio de derechos por parte de los interesados.

[denominación empresa] trasladará a la Universidad de Granada, cualquier solicitud de ejercicio de derechos de acceso, rectificación, cancelación y oposición que hubiese recibido por parte de los interesados cuyos datos sean objeto de tratamiento en el marco de la prestación del servicio, a fin de que sea resuelta por la Universidad de Granada.

Dicho traslado deberá ser inmediato, de forma que permita a la Universidad de Granada respetar los plazos legalmente establecidos de atención al ejercicio de sus derechos por parte de los interesados, asumiendo [denominación empresa] la responsabilidad que se pueda derivar del incumplimiento de dichos plazos por causa imputable a la falta o tardanza en su comunicación a la Universidad de Granada.

7. Información acerca del tratamiento.

En cumplimiento de lo dispuesto en la LOPD, queda informado de que los datos personales que en su caso sean recogidos a través de la presentación de su oferta y demás documentación necesaria para proceder a la contratación de la prestación del servicio objeto del presente contrato serán tratados por la Universidad de Granada con domicilio en Avda. del Hospicio, s/n, 18071 Granada, con la finalidad de garantizar el adecuado mantenimiento, cumplimiento y control del desarrollo del contrato.

Al objeto de mantener los datos actualizados en todo momento, el interesado deberá comunicar a la Universidad de Granada cualquier modificación en sus datos de carácter personal.

En el caso en que [denominación empresa] aporte documentos que contengan datos de carácter personal de sus trabajadores o de terceros, ya sea durante la presentación de la oferta o la ejecución del contrato, garantiza que dicha información procede de ficheros o tratamientos previamente inscritos en el Registro General de Protección de Datos y cumple todas las garantías previstas en la citada norma respecto al derecho de información y en su caso consentimiento de los interesados para llevar a cabo la cesión de datos a la Universidad de Granada.

[denominación empresa] únicamente comunicará a la Universidad de Granada datos de carácter personal adecuados, pertinentes y no excesivos en relación con las necesidades de la prestación del servicio objeto del presente contrato, garantizando que dichos datos sean exactos y puestos al día, y obligándose a comunicar a la Universidad de Granada en el plazo legalmente establecido al efecto aquellos que hayan sido rectificadas y/o deban ser cancelados según proceda.

Cualesquiera interesados podrán ejercitar sus derechos de acceso, rectificación, cancelación y oposición solicitándolo por escrito dirigido a la Secretaría General de la Universidad de Granada a la dirección anteriormente indicada.

B) Modelo de acuerdo de confidencialidad para el tratamiento de datos de carácter personal y medidas de seguridad

(Para incorporar en todo contrato de prestación de servicios ya suscrito y que no incluyese la cláusula de protección de datos y medidas de seguridad a la que se refiere el apartado A de este Anexo.)

[Lugar y Fecha]

R E U N I D O S

De una parte. La Universidad de Granada

Actúa en su nombre y representación don/doña [nombre y apellidos]

Y de otra parte. La Empresa [denominación de la empresa], con domicilio social en [dirección y localidad], provista de CIF [número]

Actúa en su nombre y representación don/doña [nombre y apellidos] en virtud del poder otorgado ante la Notaría de don/doña [nombre y apellidos] con fecha y con el número de protocolo el cual asegura que se encuentra en vigor.

E X P O N E N

I. Que la Universidad de Granada es una Institución de Derecho Público, con personalidad jurídica y patrimonio propio, a la que corresponde, en el marco de sus competencias, la prestación del servicio público de la educación superior, mediante la investigación, la docencia, el estudio, la transferencia del conocimiento a la sociedad y la extensión universitaria. Para ello, necesita que distintas empresas le presten sus servicios.

II. Que [denominación de la empresa] es una empresa que presta a la Universidad de Granada los servicios de [especificar tipo de servicios] en los términos establecidos en el contrato de servicios suscrito por ambas partes con fecha

Y en base a lo expuesto, ambas partes proceden a formalizar el presente conforme a las siguientes,

C L Á U S U L A S

Primera. Definiciones.

Cesión o comunicación de datos: Tratamiento de datos que supone su revelación a una persona distinta del interesado. A efectos del presente contrato, [denominación empresa] únicamente realizará las cesiones expresamente autorizadas y por cuenta de la Universidad de Granada, que en ese caso ostentará la condición de cedente.

Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Encargado del tratamiento: La persona jurídica o el profesional que, solo o conjuntamente con otros, trate datos personales por cuenta de la Universidad de Granada como consecuencia de una relación jurídica que le vincula con ella y delimita el ámbito de su actuación para la prestación de un servicio. A efectos del presente contrato, [denominación empresa] y aquellas empresas o profesionales que ésta precise subcontratar para el desarrollo de la prestación de los servicios contratados, tendrán la consideración de encargado del tratamiento en relación con el acceso al/los ficheros titularidad de la Universidad de Granada.

Fichero de datos: Conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso, responsabilidad de la Universidad de Granada al que accede y que es puesto a disposición de [denominación empresa] para desarrollar el servicio que esta última presta por cuenta de la Universidad de Granada.

Medidas de seguridad: Son aquellas medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal exigibles a los ficheros y tratamientos, recogidas en el Capítulo VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Nivel de seguridad: Cada uno de los niveles de seguridad (básico, medio y alto) regulados en el Capítulo VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Responsable del fichero o del tratamiento: Persona jurídica de naturaleza pública, titular del Fichero de Datos, que decide sobre la finalidad, contenido y uso del tratamiento, aunque no lo realice materialmente. A efectos del presente contrato, Universidad de Granada.

Tratamiento de datos: Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Segunda. Objeto del acuerdo.

El presente Acuerdo de Confidencialidad tiene por objeto garantizar la seguridad de la información a la que accede y trata [denominación empresa] para la prestación del servicio acordado con la Universidad de Granada, y en especial la confidencialidad, integridad y disponibilidad de los datos de carácter personal de [especificar tipo de datos] de la Universidad de Granada. De este modo, y a los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), [denominación empresa] como prestataria del servicio de [especificar servicio prestado] se convierte en encargado del tratamiento, comprometiéndose al cumplimiento de las obligaciones que le son inherentes.

Tercera. Prestaciones y propiedad de los datos.

En el contexto de la prestación de servicios encargada por la Universidad y con la finalidad mencionada, la Universidad proporciona a [denominación empresa] los datos de carácter personal relativos a [especificar tipo de datos](en adelante los «datos»), con el fin de hacer posible la prestación de los servicios encomendados. La prestación de servicios se extiende hasta el [especificar fecha].

[denominación empresa] reconoce expresamente que los datos a los que tiene acceso son de exclusiva propiedad de la Universidad de Granada, por lo que no podrá aplicarlos o utilizarlos con fines distintos a los previstos en el contrato de prestación de servicios.

[denominación empresa] únicamente tendrá acceso a aquellos datos que la Universidad de Granada le proporcione, y procederá a su tratamiento de acuerdo con las instrucciones proporcionadas no constituyendo, en ningún caso, dicho acceso una comunicación de datos, ni siquiera a efectos de su conservación; se trata exclusivamente de una simple entrega de los datos, a efectos de dar cumplimiento al contrato de servicios suscrito.

Cuarta. Tratamiento de datos.

[denominación empresa] se compromete a tratar los datos con la finalidad exclusiva de la realización del servicio. Una vez realizada la prestación del servicio, [denominación empresa] se compromete a destruir los datos proporcionados por la Universidad así como el resultado de cualquier elaboración de los mismos y los soportes o documentos en que se halle recogida la información o, en su caso, a devolvérselos a la Universidad en función de la decisión tomada por la misma en cada caso.

En caso de ser necesario que [denominación empresa] conserve los datos o una parte de los mismos a efectos de la atención de posibles responsabilidades que pudiesen derivarse del tratamiento, estos deberán

permanecer convenientemente bloqueados hasta que transcurran los plazos de prescripción correspondientes, momento en que deberán ser destruidos. La Universidad deberá tener conocimiento de ellos así como de las medidas que garanticen el adecuado bloqueo de los datos y finalmente su destrucción.

[denominación empresa] se obliga a utilizar los datos que facilite la Universidad de Granada única y exclusivamente para los fines del presente contrato y a guardar secreto profesional respecto a todos los datos de carácter personal que conozca y a los que tenga acceso durante la realización del contrato de prestación de servicios. Igualmente, se obliga a custodiar e impedir el acceso a los datos de carácter personal a cualquier tercero ajeno al presente contrato. Las anteriores obligaciones se extienden a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta de [denominación empresa] y subsistirán aun después de terminados los tratamientos efectuados en el marco del presente contrato.

[denominación empresa] se compromete a comunicar y hacer cumplir a sus empleados, asignados al proyecto, las obligaciones establecidas en los apartados anteriores.

Cualquier tratamiento de los datos que no se ajuste a lo dispuesto en el presente acuerdo, será responsabilidad exclusiva de [denominación empresa] frente a terceros y frente a la Universidad, ante la que responderá por los daños y perjuicios que le hubiere podido causar, siendo considerado también responsable del tratamiento a estos efectos.

Quinta. Medidas de seguridad

[denominación empresa] manifiesta cumplir con la normativa vigente en materia de protección de datos de carácter personal y, en particular, con las medidas de seguridad correspondientes a sus ficheros.

[denominación empresa] se compromete a aplicar a los datos facilitados por la Universidad de Granada, las medidas de seguridad de nivel [especificar el nivel de seguridad aplicable] previstas en el Capítulo VIII del Real Decreto 1720/2007, de 21 de diciembre, de acuerdo con las categorías de datos tratados. En todo caso las que se especifican en el Anexo I.

El incumplimiento de este compromiso será responsabilidad exclusiva de [denominación empresa], que responderá frente a terceros y frente a la propia Universidad de los daños y perjuicios que pudieran generarse.

Sexta. Subcesiones.

[denominación empresa] se compromete a no realizar ninguna cesión de los datos. Ello, salvo que tal cesión fuese imprescindible para la efectiva prestación del servicio, en cuyo caso, [denominación empresa] solicitará la subcesión previa autorización de la Universidad, que podrá otorgarla o resolver el contrato de servicios con [denominación empresa].

Séptima. Subcontratación.

Queda prohibida la subcontratación de todos o parte de los servicios contratados por la Universidad de Granada a [denominación empresa]. Si durante la prestación del servicio resultase necesario subcontratar todo o una parte de éste, dicha subcontratación deberá ser expresamente autorizada por la Universidad de Granada, obligándose [denominación empresa], a exigir contractualmente al subcontratista, la implementación en sus instalaciones de las medidas de seguridad previstas en el Capítulo VIII del Real Decreto 1720/2007 de 21 de diciembre, así como los demás extremos previstos en los artículos 9, 10 y 12 de la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás concordantes del citado Real Decreto que la desarrolla reglamentariamente. Dicho contrato deberá contener expresa mención a las instrucciones dictadas por la Universidad de Granada en relación con la prestación del servicio, sin perjuicio de cualesquiera otras adicionales que [denominación empresa] exija al subcontratista en el marco de las establecidas por la Universidad de Granada. A estos efectos el subcontratista será considerado encargado del tratamiento.

(En caso de ser conocida previamente la necesidad de subcontratación dicha cláusula será sustituida por la siguiente):

La Universidad de Granada, autoriza expresamente y mediante la presente estipulación, a [denominación empresa], la cual acepta, a subcontratar los siguientes servicios:

Lo que supone el tratamiento de los datos contenidos en los ficheros denominados «[incluir el nombre de los ficheros accedidos]», a las entidades [denominación subcontratista 1] y/o [denominación subcontratista 2], obligándose [denominación empresa], a exigir contractualmente a éstas, la implementación en sus instalaciones de las medidas de seguridad previstas en el Capítulo VIII del Real Decreto 1720/2007, de 21 de diciembre, así como los demás extremos previstos en los artículos 9, 10 y 12 de la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás concordantes del citado Real Decreto que la desarrolla

reglamentariamente. Dicho contrato deberá contener expresa mención a las instrucciones dictadas por la Universidad de Granada en relación con la prestación del servicio, sin perjuicio de cualesquiera otras adicionales que [denominación empresa] exija al subcontratista en el marco de las establecidas por la Universidad de Granada. A estos efectos el subcontratista será considerado encargado del tratamiento.

Octava. Ejercicio de derechos por parte de los interesados

[denominación empresa] trasladará a la Universidad de Granada, cualquier solicitud de ejercicio de derechos de acceso, rectificación, cancelación y oposición que hubiese recibido por parte de los interesados cuyos datos sean objeto de tratamiento en el marco de la prestación del servicio, a fin de que sea resuelta por la Universidad de Granada.

Dicho traslado deberá ser inmediato, de forma que permita a la Universidad de Granada respetar los plazos legalmente establecidos de atención al ejercicio de sus derechos por parte de los interesados, asumiendo [denominación empresa] la responsabilidad que se pueda derivar del incumplimiento de dichos plazos por causa imputable a la falta o tardanza en su comunicación a la Universidad de Granada.

Novena. Información acerca del tratamiento.

En cumplimiento de lo dispuesto en la LOPD, queda informado de que los datos personales que, en su caso, se recogieron a través de la presentación de su oferta y demás documentación necesaria para proceder a la contratación de la prestación del servicio al que se refiere el presente acuerdo, serán tratados por la Universidad de Granada con domicilio en Avda. del Hospicio, s/n, 18071 Granada, con la finalidad de garantizar el adecuado mantenimiento, cumplimiento y control del desarrollo del contrato.

Al objeto de mantener los datos actualizados en todo momento, el interesado deberá comunicar a la Universidad de Granada cualquier modificación en sus datos de carácter personal.

En el caso en que [denominación empresa] aporte documentos que contengan datos de carácter personal de sus trabajadores o de terceros, ya sea durante la presentación de la oferta o la ejecución del contrato, garantiza que dicha información procede de ficheros o tratamientos previamente inscritos en el Registro General de Protección de Datos y cumple todas las garantías previstas en la citada norma respecto al derecho de información y en su caso consentimiento de los interesados para llevar a cabo la cesión de datos a la Universidad de Granada.

[denominación empresa] únicamente comunicará a la Universidad de Granada datos de carácter personal adecuados, pertinentes y no excesivos en relación con las necesidades de la prestación del servicio objeto del presente contrato, garantizando que dichos datos sean exactos y puestos al día, y obligándose a comunicar a la Universidad de Granada en el plazo legalmente establecido al efecto aquellos que hayan sido rectificadas y/o deban ser cancelados según proceda.

Cualesquiera interesados podrán ejercitar sus derechos de acceso, rectificación, cancelación y oposición solicitándolo por escrito dirigido a la Secretaría General de la Universidad de Granada a la dirección anteriormente indicada.

Décima. Entrada en vigor y duración.

El presente Acuerdo de Confidencialidad entrará en vigor en la fecha de su firma, y su duración se extenderá durante la vigencia del contrato de servicios suscrito entre ambas partes con fecha . Este compromiso de confidencialidad formará parte del contrato de servicios existente entre ambas partes.

Don/doña [nombre y apellidos]

[nombre y apellidos]

Universidad de Granada

[denominación empresa]

Anexo al Acuerdo de Confidencialidad. Medidas de seguridad aplicables en el tratamiento de datos de carácter personal

Las medidas de seguridad aplicables por [denominación empresa] en el tratamiento de datos de carácter personal serán como mínimo las establecidas en el presente Anexo, en función de los datos objeto de tratamiento y del nivel de medidas de seguridad que se especifique en el Acuerdo de Confidencialidad de tratamiento de datos del que el presente Anexo forma parte.

En el caso en que durante la prestación del servicio [denominación empresa] acceda y trate datos de nivel básico, se compromete al cumplimiento de las medidas de seguridad recogidas en los artículos 85 a 94 y 105 a 108 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en lo sucesivo RDLOPD), y en todo caso las siguientes:

a) En el caso en que el servicio sea prestado en los locales de la [denominación empresa], ésta dispondrá de un Documento de Seguridad de obligado cumplimiento en el que se recogerán las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente.

b) El personal de [denominación empresa] conocerá sus deberes de custodia y confidencialidad respecto a los datos o la documentación que tengan a su cargo, sus funciones y obligaciones, así como las normas de seguridad que afectan al desarrollo de las mismas, encontrándose claramente definidas y documentadas.

c) En el caso en que el tratamiento se realice en los sistemas de [denominación empresa], ésta dispondrá de mecanismos para identificar y autenticar de forma inequívoca y personalizada a los usuarios del sistema, y si la autenticación está basada en contraseñas, éstas caducarán periódicamente y serán almacenadas de forma ininteligible.

d) El sistema tendrá establecidos perfiles de acceso que permitirán, en atención a la asignación de obligaciones y responsabilidades relacionadas con el tratamiento de datos de carácter personal, que cada usuario acceda únicamente a aquellos recursos que precise para el desarrollo de sus funciones. La asignación del perfil y otorgamiento del acceso se hará mediante un procedimiento documentado y auditable.

e) Si los sistemas empleados en el tratamiento fuesen propiedad de la Universidad de Granada, [denominación empresa] adoptará los mecanismos de control implantados por ésta, comprometiéndose el personal de la [denominación empresa] al cumplimiento de las medidas y procedimientos asociados al mismo.

f) [denominación empresa] mantendrá un registro de las incidencias, acorde a lo establecido en el artículo 90 del RDLOPD, que puedan afectar a la seguridad de los datos de carácter personal. [denominación empresa] comunicará a la Universidad de Granada un resumen de las incidencias acaecidas, con la periodicidad que se establezca.

g) Si los sistemas empleados en el tratamiento fuesen propiedad de la Universidad de Granada, el personal de [denominación empresa] utilizará el sistema de notificación de incidencias de la Universidad de Granada, y se preocupará de que su personal conozca su responsabilidad en la notificación, considerándose el conocimiento y la no notificación de una incidencia como una falta contra la seguridad.

h) [denominación empresa] dispondrá de procedimientos de copias diarias, y de recuperación que puedan garantizar la reconstrucción en el estado en que se encontraban los datos en caso de producirse su pérdida o destrucción. La correcta definición, funcionamiento y aplicación de dichos procedimientos se verificará cada seis meses, quedando registro de dichas verificaciones.

i) Si la prestación de servicios objeto del contrato del que este documento trae causa conlleva la creación de soportes informáticos o en papel con datos de carácter personal, estarán sujetos a procedimientos de identificación, inventario y almacenamiento de acuerdo con criterios de archivo definidos y acceso restringido. Las salidas de dichos soportes y documentos estarán autorizadas de acuerdo con relaciones de responsables debidamente designados, disponiendo [denominación empresa] de mecanismos de destrucción de soportes y documentos, de forma que se evite su recuperación posterior.

j) En dicho caso el traslado de soportes y documentos que contengan datos de carácter personal, se realizará protegido de forma que se evite su sustracción, pérdida, manipulación o acceso indebido.

k) Si fuese necesario realizar una parte del tratamiento fuera de los locales de la [denominación empresa] incluso mediante el uso de dispositivos portátiles, dicha actuación será autorizada de acuerdo con relaciones de responsables debidamente designados.

l) Las transmisiones y accesos a través de redes de telecomunicaciones se realizarán con medidas que garanticen un nivel de seguridad equivalente a los accesos en modo local.

m) No se realizarán pruebas con datos reales procedentes de los ficheros titularidad de la Universidad de Granada, salvo que ésta lo autorice expresamente, debiendo en ese caso respetar durante el proceso las medidas de seguridad acordes al nivel de seguridad que corresponda a las categorías de datos empleados. Dicho proceso se reflejará en un registro.

Si durante la prestación del servicio [denominación empresa] accediese y tratase datos de carácter personal de nivel medio, además del cumplimiento de lo ya expuesto, garantiza tener implantadas las medidas de seguridad recogidas en los artículos 95 a 100, 109 y 110 del RDLOPD, y en todo caso las siguientes:

a) Los mecanismos de acceso a los sistemas donde se estén tratando datos de carácter personal por cuenta de la Universidad de Granada, impedirán intentar reiteradamente un acceso no autorizado.

b) Si la prestación de servicios objeto del contrato del que este documento trae causa conllevara la creación de soportes informáticos o en papel con datos de carácter personal y fuese necesario su traslado, [denominación empresa] contará con sistemas de registro de entradas y salidas acordes a lo establecido en el artículo 97 del RDLOPD.

c) Los procedimientos de recuperación de datos requerirán autorización de la Universidad de Granada y quedarán debidamente registrados.

d) [denominación empresa] habrá designado al menos un Responsable de Seguridad encargado de coordinar y controlar las medidas de seguridad aplicables a los tratamientos de datos de carácter personal, sin perjuicio de la coordinación llevada a cabo por el responsable de seguridad designado por la Universidad de Granada para lo cual recibirá la información de control que periódicamente le deba ser facilitada por [denominación empresa].

e) [denominación empresa] contará con medidas de acceso físico que impidan a toda aquella persona que no esté convenientemente autorizada el acceso a los lugares donde se encuentran los equipos.

f) La Universidad de Granada podrá realizar auditorías de los sistemas de información [denominación empresa], donde se estén realizando los tratamientos de datos de carácter personal, con el fin de verificar el cumplimiento de las medidas recogidas en el presente Anexo, al menos cada dos años, siempre que se hagan de forma que no se altere el adecuado desarrollo de la prestación del servicio contratado.

En el caso en que durante la prestación del servicio [denominación empresa] acceda y trate datos de nivel alto, se compromete al cumplimiento de las medidas de seguridad recogidas en los artículos 101 a 104 y 111 a 114 del RDLOPD, y en todo caso las siguientes:

a) Los sistemas de [denominación empresa] empleados para el tratamiento de datos de carácter personal, dispondrán de mecanismos de registro de cualquier acceso que se produzca a datos considerados especialmente protegidos por la LOPD y así como a cualquier tipo de dato al que se le asigne un nivel alto de medidas de seguridad. Dichos registros se conservarán al menos durante dos años. En caso de detectar incidencias en la información de control registrada [denominación empresa] se lo comunicará a la Universidad de Granada.

b) Si la prestación de servicios objeto del contrato del que este documento trae causa conlleva la creación de soportes informáticos o en papel con datos de carácter personal, su método de etiquetado se realizará con sistemas de codificación debidamente custodiados que impidan identificar su contenido a terceros. Dichos soportes y documentos se almacenarán protegidos, en áreas de acceso restringido que quedará debidamente registrado.

c) En dicho caso, estará controlada la reproducción de información con datos de carácter personal y sometida a procesos de destrucción una vez finalizado su uso.

d) El traslado de datos de carácter personal fuera de las instalaciones de [denominación empresa] donde se esté realizando el tratamiento, en soportes informáticos o en ordenadores portátiles se realizará cifrando dichos datos o con un mecanismo que ofrezca garantías similares.

e) [denominación empresa] dispondrá al menos de dos juegos de copias de seguridad y procedimientos de recuperación de los datos de carácter personal, debiendo almacenarse uno de ellos debidamente protegido, en una ubicación protegida y suficientemente alejada del Centro de Proceso de Datos de forma que se garantice su recuperación en caso de tener lugar una incidencia importante.

f) La transmisión de datos de carácter personal a través de redes de comunicaciones públicas o inalámbricas se hará cifrado mediante mecanismo similar.