GUÍA PARA EL TRATAMIENTO DE DATOS PERSONALES DE VÍCTIMAS DE VIOLENCIA CONTRA LAS MUJERES

EMAKUNDE
EMAKUMEAREN EUSKAL ERAKUNDEA
INSTITUTO VASCO DE LA MUJER
Eusko Jaurlaritzako Erakunde Autonomiaduna
Organismo Autónomo del Gobierno Vasco

GUÍA

30

EMAKUNDE
INSTITUTO VASCO DE LA MUJER
VITORIA - GASTEIZ 2015

GUÍA PARA EL TRATAMIENTO DE DATOS PERSONALES DE VÍCTIMAS DE VIOLENCIA CONTRA LAS MUJERES

TÍTULO: "Guía para el tratamiento de datos personales de víctimas de violencia contra las mujeres"
EDITA: Emakunde-Instituto Vasco de la Mujer
AUTORA: Ticdatum SLU
DISEÑO GRÁFICO Y MAQUETACIÓN: Arrin. Comunicacion y Diseño
FECHA: Noviembre 2015
DESCRIPTORES: Violencia de género, víctimas, malos tratos, protección de datos personales, normativa, guías

ÍNDICE

PRESENTACIÓN 9

MARCO LEGAL 13

a) Legislación aplicable 15

b) Coordinación institucional y protección de datos 16

c) La violencia contra las mujeres en la LOPD 16

1. INFORMACIÓN Y RECOGIDA DE DATOS PERSONALES 19

CUANDO UNA VÍCTIMA DE LA VIOLENCIA CONTRA LAS MUJERES SE ACERCA A UN SERVICIO DE ATENCIÓN O ASESORAMIENTO: ¿DE QUÉ INFORMO A LA PERSONA Y QUÉ DATOS PERSONALES RECOJO? 21

- Primera cuestión: ¿Cuál es el contenido de la información que hay que ofrecer a una mujer que enfrenta violencia? 21
- Segunda cuestión: ¿Qué problemas se plantean en función del medio utilizado por una mujer que enfrenta violencia para ponerse en contacto con los servicios de atención? 23
- Tercera cuestión: ¿Qué datos puedo solicitar a una mujer víctima de violencia? . 26
- Cuarta cuestión: ¿Cómo recojo los datos personales de la mujer víctima de violencia? 27

2. TRATAMIENTO DE DATOS PERSONALES 31

UNA VEZ RECOGIDOS LOS DATOS PERSONALES DE LAS VÍCTIMAS DE VIOLENCIA CONTRA LAS MUJERES, ¿QUÉ PUEDO HACER CON ELLOS? EL TRATAMIENTO DE LOS DATOS PERSONALES 33

- Primera cuestión: ¿Todo el personal de un organismo de atención a la mujer víctima de violencia tiene acceso a los datos personales? 33

- Segunda cuestión: ¿Podemos destinar los datos personales recabados a otras finalidades distintas para las que se recogieron inicialmente? 34
- Tercera cuestión: ¿Cómo garantizamos la confidencialidad de datos personales en procesos de concurrencia pública? 35
- Cuarta cuestión: ¿Podríamos utilizar los datos personales de las mujeres víctimas de violencia para finalidades estadísticas? 37

3. CESIÓN DE DATOS PERSONALES 39

CÓMO COMUNICAR A TERCERAS PERSONAS LOS DATOS PERSONALES RELACIONADOS CON LA VIOLENCIA CONTRA LAS MUJERES. LA CESIÓN DE LOS DATOS PERSONALES 41

- Primera cuestión: ¿Se pueden ceder datos de una mujer víctima de violencia a otras personas o entidades? 41
- Segunda cuestión: ¿Es posible la cesión de datos personales entre personas o entidades que integran un protocolo de colaboración para la atención integral a mujeres víctimas de violencia? 42
- Tercera cuestión: ¿Se pueden ceder a los servicios sociales, o entre distintas áreas de servicios sociales, datos personales de una persona menor de edad que viva en una supuesta situación de violencia? 44
- Cuarta cuestión: ¿Puede facilitarse información de carácter personal por vía telefónica? 45

4. SEGURIDAD DE DATOS PERSONALES 47

LA SEGURIDAD DE LOS DATOS PERSONALES: CÓMO DEBEMOS CUSTODIAR LOS DATOS DE LAS MUJERES VÍCTIMAS DE LA VIOLENCIA. 49

- Primera cuestión: ¿cuáles son las precauciones o medidas de seguridad que hay que adoptar en relación con los datos personales de las mujeres víctimas de violencia? 49
- Segunda cuestión: ¿Tengo que adoptar medidas específicas de seguridad dependiendo del medio por el que han llegado los datos personales? 54

- Tercera cuestión: ¿Es posible la elaboración por el personal de ficheros paralelos a las bases de datos corporativas para un mejor manejo de los datos personales de las mujeres víctimas de violencia? 55
- Cuarta cuestión: ¿Cuál es el uso razonable de los sistemas de información por el personal que interviene en los procesos de atención? 56

5. PERIODO DE CONSERVACIÓN O UTILIZACIÓN DE DATOS PERSONALES 59

UNA VEZ QUE SE HAN UTILIZADO LOS DATOS PERSONALES DE MUJERES VÍCTIMAS DE VIOLENCIA, ¿HASTA CUÁNDO SE PUEDE GUARDAR O UTILIZAR SUS DATOS PERSONALES? 61

6. GARANTÍA DE LOS DERECHOS ARCO 63

¿CÓMO SE GARANTIZA EL EJERCICIO DE LOS DERECHOS ARCO? 65

- Primera cuestión: ¿Cuándo debemos informar a la mujer que enfrenta violencia de sus derechos en relación con el tratamiento que se hace de sus datos personales? 65
- Segunda cuestión: ¿Qué proceso debemos seguir ante el ejercicio de derecho personal ARCO? 66

7. RESUMEN 69

8. BIBLIOGRAFÍA Y DOCUMENTACIÓN 73

9. GLOSARIO DE TÉRMINOS 81

ANEXOS 87

ANEXO 1: CLÁUSULA DE CONSENTIMIENTO INFORMADO PARA LA RECOGIDA Y CESIÓN DE DATOS PERSONALES 89

ANEXO 2: FAQ-PREGUNTAS FRECUENTES PLANTEADAS POR EL PERSONAL TÉCNICO EN EL PROCESO DE EJECUCIÓN DE LA GUÍA 93

1. Información y recogida de datos personales 93

2. Tratamiento de datos personales 94

3. Cesión de datos personales. 108

4. La seguridad de los datos personales. 115

ANEXO 3: La cesión de datos en la atención a las personas menores de edad ante situaciones de violencia contra las mujeres. 117

1. Normativa para la protección de los y las menores de edad. 117

2. Interpretación de la normativa para la protección de los y las menores de edad en relación a la ley orgánica para la protección de datos personales. 118

3. Resumen: los y las menores de edad y la protección de datos. 122

PRESENTACIÓN

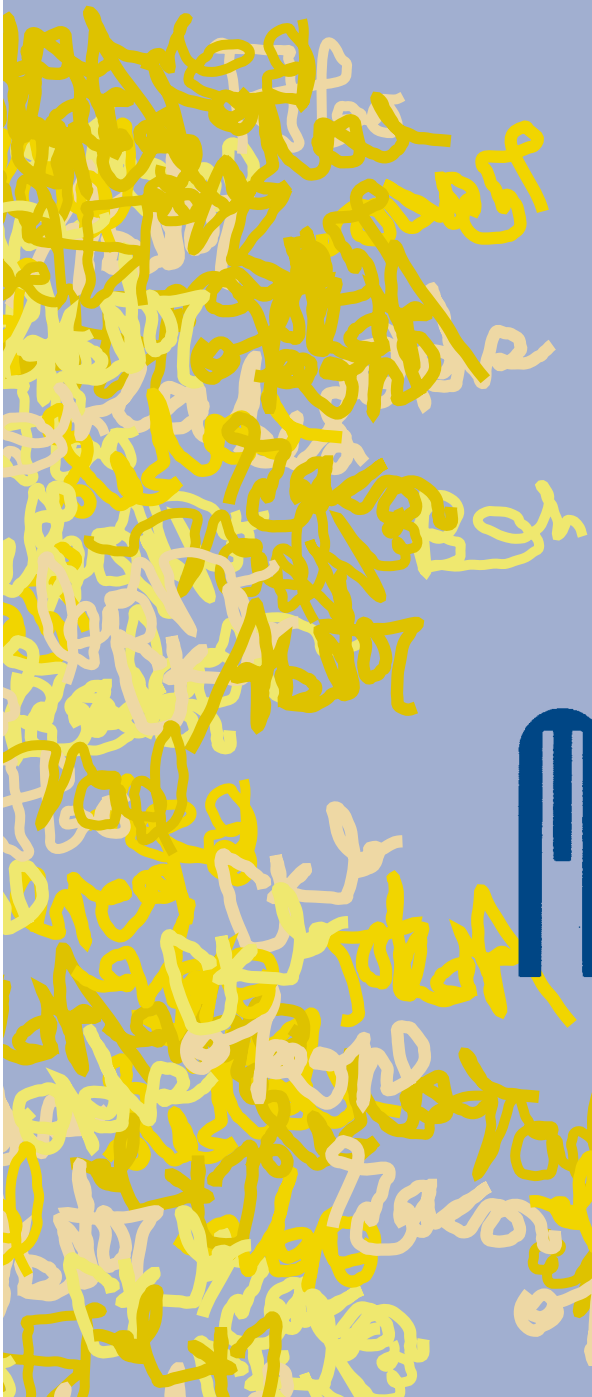
Garantizar el derecho de las mujeres a una vida libre de violencia requiere una actuación coordinada y eficaz entre los distintos servicios que prestan atención a las mujeres que la sufren. Con el objetivo de estrechar la coordinación institucional en la materia, las instituciones del País Vasco firmaron el 3 de febrero de 2009 el II Acuerdo Interinstitucional para la mejora en la atención a mujeres víctimas de maltrato en el ámbito doméstico y de violencia sexual, y, así mismo, diferentes municipios del país han firmado protocolos de coordinación interinstitucional.

La coordinación institucional requiere en muchos casos guardar/ceder/comunicar datos, por lo que es importante medir cómo se realizan estas acciones con el objetivo de garantizar la privacidad de las mujeres que acuden a las instituciones y teniendo en cuenta la manera en la que inciden la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la misma.

Esta guía resuelve el diálogo entre estos dos mandatos: el deber de coordinación para ofrecer una atención que facilite el proceso de recuperación, por un lado; y el deber de respetar las decisiónes de las mujeres en estos procesos, así como de garantizar a las mujeres el control de los datos sobre su persona. Así, este documento pretende orientar la coordinación eficaz garantizando el respeto a la protección de los datos de las mujeres víctimas de violencia. Y en este sentido, queremos dar las gracias por su colaboración a la Agencia Vasca de Protección de Datos.

Somos conscientes de que las cuestiones planteadas no son fáciles de dirimir y esperamos que esta guía ayude a conocer cómo, en el marco actual, debemos coordinarnos entre las instituciones respetando, también, las demandas de una protección de datos efectiva. Debemos, en cualquier caso, seguir avanzando en el debate y análisis de estas cuestiones para asegurar que este contexto responde a las demandas de las mujeres que luchan para acceder al derecho fundamental de vivir sin ser agredidas.

Miren Izaskun Landaida Larizgoitia
Directora de Emakunde-Instituto Vasco de la Mujer



MARCO LEGAL

MARCO LEGAL

A) LEGISLACIÓN APLICABLE

La presente guía ha tenido en cuenta la legislación vigente en materia de protección de datos personales y seguridad de la información aplicable al tratamiento de la información personal de las mujeres víctimas en violencia a que se hace referencia y, en particular, la que a continuación se relaciona:

— Declaración Universal de los Derechos Humanos de 10 de diciembre de 1948.

— Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

— Ley 4/1986, de 23 de abril, de Estadística de la Comunidad Autónoma de Euskadi.

— Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

— Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

— Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

— Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico.

— DIRECTIVA 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

— Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

— Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género.

— Ley 4/2005, de 18 de febrero, para la Igualdad de Mujeres y Hombres.

— Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

— Instrumento de ratificación del Convenio del Consejo de Europa sobre Prevención y Lucha contra la Violencia contra la Mujer y la Violencia Doméstica hecho en Estambul, el 11 de mayo de 2011.

— Directiva 2012/29/UE del Parlamento Europeo y del Consejo de 25 de octubre de 2012 por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos, y por la que se sustituye la Decisión marco 2001/220/JAI del Consejo.

— Reglamento (UE) nº 611/2013 de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas.

Esta normativa se ha examinado en el marco proyectado por el II Acuerdo Interinstitucional para la Mejora en la Atención a Mujeres Víctimas de Maltrato en el Ámbito Doméstico y de Violencia Sexual, como respuesta institucional al problema de la violencia contra las mujeres estableciendo los mecanismos necesarios para la mejora de la coordinación entre las instituciones implicadas en la Comunidad Autónoma de Euskadi en la asistencia a las mujeres víctimas de maltrato en el ámbito doméstico y de violencia sexual.

B) COORDINACIÓN INSTITUCIONAL Y PROTECCIÓN DE DATOS

En este contexto, el objetivo de la presente guía para el tratamiento de datos personales de mujeres que enfrentan violencia es la coordinación institucional eficiente en este marco con pleno respeto a la protección de datos de carácter personal.

El planteamiento requiere, dentro de los márgenes posibilitados por la legislación, una actuación coordinada entre los distintos sectores de intervención de la administración pública vasca implicados en la atención a este colectivo desde la perspectiva de la protección de datos de carácter personal que, dentro de los márgenes de la ley, permita integrar las distintas actuaciones de los ámbitos participantes en la tutela y protección de los derechos de las víctimas de la violencia contra las mujeres.

La normativa de protección de datos es un medio que contribuye a proteger la seguridad de la mujer y de sus derechos para evitar que a la conmoción producida por el daño físico, psíquico, familiar social o económico experimentado por las víctimas afectadas por actuaciones reprobables de violencia, se añada una segunda victimización derivada de un inadecuado tratamiento de su información personal en la ejecución de los procesos que la administración destina a la atención y tutela de su situación.

Ello exige diseñar un escenario de actuación adecuado para garantizar la protección de datos en términos positivos que conduzca a fijar la opción más favorable. Esta opción debe permitir, a todas las personas intervinientes en los procesos de atención a las mujeres que enfrentan violencia, desarrollar una intervención respetuosa en el ámbito del tratamiento de su información personal.

C) LA VIOLENCIA CONTRA LAS MUJERES EN LA LOPD

Conforme a la normativa actual es el artículo 81.3 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) el que otorga el máximo nivel de protección a los datos personales derivados de los actos de violencia de género, estableciendo expresamente que "Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal: c) Aquéllos que contengan datos derivados de actos de violencia de género."

Así, hay que señalar que las obligaciones impuestas en el ámbito de la violencia contra las mujeres por la normativa de protección de datos se refieren específicamente al contenido del art. 1 de la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género; esto es, la violencia ejercida sobre las mujeres por parte de quienes sean o hayan sido sus cónyuges o de quienes estén o hayan estado ligados a ellas por relaciones similares de afectividad, aun sin convivencia. Ello comprende las violencias físicas y psicológicas, incluidas las agresiones a la libertad sexual, las amenazas, las coacciones o la privación arbitraria de libertad.

Este ámbito subjetivo no impide, sino que además aconseja, su aplicación a todas las formas de violencia contra las mujeres como manifestación de la discriminación, situación de desigualdad y las relaciones de poder de los hombres sobre las mujeres, ejercida sobre éstas por el mero hecho de serlo, y que tenga como consecuencia, o que tenga posibilidades de tener como consecuencia, un perjuicio o sufrimiento de la salud física, sexual o psicológica de una mujer. Máxime si se tiene en cuenta que en todos estos escenarios de violencia contra las mujeres, se pondrán de manifiesto datos de salud, ideología, religión, creencias u origen racial que, al igual que los datos de violencia de género, son datos de especial sensibilidad que gozan del mayor nivel de protección que la normativa de protección de datos establece para el amparo, custodia y defensa de la información personal.

Precisamente, en esa línea integradora de la protección a las mujeres contra las que se ejerce algún tipo de violencia sexista se encuentra el II Acuerdo Interinstitucional para la Mejora en la Atención a Mujeres Víctimas de Maltrato en el Ámbito Doméstico y de Violencia Sexual.

Por lo tanto, a lo largo de la presente guía todos los escenarios de violencia ejercida contra las mujeres serán objeto de integración en el adecuado tratamiento de los datos personales contenido en la presente guía.

1. NFORMACIÓN Y RECOGIDA DE DATOS

1. CUANDO UNA VÍCTIMA DE LA VIOLENCIA CONTRA LAS MUJERES SE ACERCA A UN SERVICIO DE ATENCIÓN O ASESORAMIENTO: ¿DE QUÉ INFORMO A LA PERSONA Y QUÉ DATOS PERSONALES RECOJO?

PRIMERA CUESTIÓN:

¿CUÁL ES EL CONTENIDO DE LA INFORMACIÓN QUE HAY QUE OFRECER A UNA MUJER QUE ENFRENTA VIOLENCIA?

Las mujeres víctimas de violencia a los que se soliciten datos personales deberán ser previamente informadas de modo expreso, preciso e inequívoco de los siguientes aspectos:

a) De que los datos facilitados serán incorporados a un fichero (con la denominación expresa de dicho fichero), así como de la finalidad de la recogida de tales datos y de las personas, físicas o jurídicas, destinatarias de la información.

b) De que tienen el deber de facilitar los datos reales que le sean solicitados de manera leal y verdadera, así como el de colaborar en su obtención, especialmente cuando sean necesarios con motivo de la asistencia sanitaria o por razones de interés público.

c) De las consecuencias de facilitar los datos o de la negativa a suministrarlos; esto es, que aportar los datos solicitados servirá para identificar la atención necesitada y los recursos disponibles para abordar esa atención, mientras que su negativa impedirá determinar correctamente esas necesidades y sus correspondientes recursos.

d) De la posibilidad de ejercitar los derechos ARCO- de acceso, rectificación, cancelación y oposición- en las condiciones legalmente establecidas.

e) De cuál es la identidad y dirección de la organización, entidad o servicio responsable del fichero o, en su caso, de su representante, ante el que poder ejercitar los referidos derechos de acceso, rectificación, cancelación y oposición.

Esta información deberá facilitarse de forma comprensible y adecuada. Además, no basta con informar sino que debemos poder acreditar que se ha cumplido con este deber de información para que, en el caso de que la persona niegue haber autorizado una utilización concreta de sus datos personales podamos verificar que contamos con esa autorización, así como, para el caso de que solicite un acceso a la información personal que le pertenece y que manejamos podamos darle la información precisa acerca de la finalidad para la que la esta-

mos utilizando y a qué persona u organización, por ejemplo, se la hemos cedido. Por lo tanto, es necesario conservar algún elemento con el que poder acreditar el cumplimiento del deber de información a la mujer. Para ello es aconsejable incluir en el formulario de recogida, sea cual fuere el medio de obtención de la información (escrito, web, App) que se ha cumplido con la obligación de información descrita.

En caso de menores de edad el consentimiento pertenece a la persona mayor de 14 años. Si esta persona se encuentre física o jurídicamente incapacitada se le informará en función de su grado de comprensión, sin perjuicio de informar también a su representante legal, tutor o tutora.

En definitiva, el personal debe ofrecer a las víctimas de violencia información suficiente y adecuada en relación con los datos que se van a recoger, para qué finalidad se van a recoger y cómo se van a guardar, añadiendo una información sobre quién es el servicio o la persona responsable de que se utilicen correctamente.

Es muy importante que las técnicas y técnicos que intervienen en el proceso de atención expliquen la finalidad de dicha recogida; esto es, para qué se recogen esos datos: la finalidad puede ser de atención, curativa (en el caso de médicos y médicas y personal sanitario), persecución del delito (en el caso de la policía), u otras.

Este requisito exige primero una reflexión sobre los datos que se recogen, dado que dependiendo de la finalidad, los datos personales a recabar podrán ser más o menos numerosos. No es posible recoger datos que no estén ajustados a la finalidad. Por ejemplo, no es posible recoger datos económicos si la finalidad es curativa.

Sea cual fuere el medio o medios utilizados para la recogida de información, también se comunicará a las mujeres a quienes se atiende la denominación del fichero en el que se van a guardar los datos personales recogidos, que debe estar creado e inscrito con anterioridad a esta recogida en el registro de la Agencia de Protección de Datos competente; que en el caso de las instituciones públicas vascas es la Agencia Vasca de Protección de Datos (AVPD). También se debe comunicar la identidad de quién es responsable del fichero y ante quién puede la mujer víctima de violencia ejercitar sus derechos ARCO.

Los denominados derechos ARCO son el conjunto de derechos - de acceso, de rectificación, de cancelación y de oposición)- a través de los cuales la LOPD garantiza a las personas el poder de control sobre sus datos personales. Esta cuestión cobra especial importancia dado que se da con frecuencia el caso de mujeres que han sido víctimas de violencia y resuelto el problema no desean permanecer en los ficheros oficiales, y manifiestan su deseo de cancelación de esos datos e incluso de oposición a su tratamiento. En este caso, habrá que resolver el ejercicio de este derecho pasando por analizar la previsión de finalidad futura de esa información para retenerla y no cancelar los datos; esto es, cancelarlos cuando se agote la finalidad por la que se recogieron.

Además, hay que informarle que los datos que se entreguen serán confidenciales y sólo serán tratados por aquellas personas autorizadas y que tengan una relación con la finalidad para la que fueron recabados sus datos.

Y, finalmente, si existe la intención de realizar cesiones de estos datos a otras administraciones públicas o a otras personas u organizaciones privadas, la persona debe ser informada de este aspecto en el momento de la recogida de los datos, y debe dársele la opción de dar su consentimiento para ello o no darlo. Esta opción es esencial para que las cesiones futuras puedan ser acordes a la ley.

Analizaremos esta cuestión posteriormente, simplemente aquí debemos dejar constancia de que en la recogida de datos personales se debe incluir la información sobre dichas cesiones de datos.

SEGUNDA CUESTIÓN:

¿QUÉ PROBLEMAS SE PLANTEAN EN FUNCIÓN DEL MEDIO UTILIZADO POR UNA MUJER QUE ENFRENTA VIOLENCIA PARA PONERSE EN CONTACTO CON LOS SERVICIOS DE ATENCIÓN?

Las posibilidades que existen a priori y que condicionan la recogida de información, son las siguientes:

a) Teléfono

b) Presencial

c) Correo electrónico

d) Página web

e) Aplicaciones móviles diseñadas para este contacto.

En función de cuál sea la forma de acudir al servicio de atención o asesoramiento, los requisitos y también los problemas son distintos.

A) TELÉFONO

Si se plantea la recogida por teléfono de datos personales la atención telefónica la debe realizar personal que, además de una formación específica para dicha atención, tenga una formación básica en relación a la materia de la protección de datos. Esto requiere que pueda dar una explicación adecuada sobre estas cuestiones antes de proceder a recoger información.

Como punto de partida, no es una práctica aconsejable recoger datos personales por este medio sino convocar a la persona a una cita con el personal técnico que la atenderá ofreciéndole la información que requiere su atención y también, como un contenido más, la información relativa a la protección de sus datos personales. Sin embargo, siquiera la mera fijación de una cita exige conocer los datos que permitan identificar y localizar a esa persona -datos básicos de identidad, domicilio y/o teléfono), datos que constituyen información personal.

Para lograr este propósito, un contenido verbal básico supone informar a la mujer que sus datos van a ser tratados de forma confidencial, que van a ser recogidos al objeto de poder prestarle la atención adecuada, que si no indicara esos datos no podría prestársele esa atención y que se le ofrecerá información más detallada en la cita a la que se persone para que esté absolutamente tranquila en la seguridad, cuidado y respeto con los que se emplearán sus datos personales. De ese modo, una vez atendida presencialmente la persona se pasaría a cumplir el primer estadio dirigido a la protección de sus datos personales que es el consentimiento informado del tratamiento, uso y manejo de sus datos, y se analiza a continuación.

B) PRESENCIAL

Si la recogida de información es presencial, se informará de forma particular y expresa a la mujer de los extremos que exige la ley antes de recoger la información (1). Esta información se hará una sola vez, no siendo necesario reiterar esta información cada vez que la misma persona acuda al servicio de atención a este colectivo.

En concreto, y ante la cláusula de consentimiento informado para la recogida y cesión de datos personales, se le indicará qué datos se van a recoger. Bastará para ello realizar una aproximación a los mismos o una descripción general de cuáles son estos datos (datos personales básicos de identidad, datos económicos, datos de salud, datos sobre la familia y la convivencia, datos sobre sus hijos o hijas y su situación, entre otros, que sea necesario recabar), se le indicará que la finalidad de la recogida de esos datos es poder ofrecerle una atención integral y adecuada a sus necesidades, y que para ello será en ocasiones necesario comunicar esa información a otras personas o entidades.

En este punto, la técnica o técnico que le asesora marcará las casillas de la cláusula de consentimiento informado correspondientes a las personas, organismos o entidades a los que, por motivo de la finalidad asistencial que requiera cada mujer, serán o podrán ser cedidos sus datos personales. Completada ésta, el documento será firmado por la mujer a quien, a continuación, se entregará una copia. En el caso de que la persona esté impedida para la firma, por la razón que fuere, podrá ser firmada por la persona que la mujer indique a tal efecto.

(1) Ver Anexo 1: Cláusula de consentimiento informado para la recogida y cesión de datos personales.

C) CORREO ELECTRÓNICO

Si la recogida de información se realiza por correo electrónico, es decir, se pone a disposición de las mujeres víctimas de violencia un correo para denuncia, atención, ayuda u otras finalidades, hay que tener en cuenta que las mujeres lo podrían utilizar para facilitar a la administración que gestione este correo información que incluya datos personales.

Por ello debe diseñarse un sistema que permita informar a la mujer y recoger su consentimiento, sea mediante la respuesta automática a cualquier correo que se envíe, sea mediante la puesta en contacto lo antes posible con la mujer víctima de violencia para ser informada y recoger su consentimiento, sea mediante la ubicación en la página web, donde se facilita el correo de una cláusula que sea imprescindible leer antes de poder enviar el correo, y que facilite a la administración una "huella" de su lectura y del consentimiento de la mujer víctima de violencia.

D) PÁGINA WEB

Muy cercana a esta última solución es la que debemos dar a la recogida de información vía página web. Si se ha diseñado un formulario que hay que rellenar por la mujer víctima de violencia donde se recogen datos personales, habrá que incluir una cláusula de información con los parámetros antes expuestos, y un apartado donde esta mujer pueda optar por dar o no su consentimiento. El diseño del sistema tiene que ser de tal forma que si la mujer no da su consentimiento el formulario no pueda ser enviado, informándole de las consecuencias de su negativa. Esto exigirá un esfuerzo de diseño en la página web.

No obstante, y dada la especial sensibilidad que requiere este colectivo, la opción para el caso en que la mujer no desee expresar ese consentimiento el sistema deberá generar una alerta que permita conocer la existencia de una mujer que muestra interés o necesidad de atención para, posteriormente y de forma presencial, recabar el consentimiento. La valoración de la urgencia requerirá una atención inmediata e inaplazable sin perjuicio de recabar posteriormente sus datos, tal y como se actuaría en cualquier otra situación que no fuera la atención vía web. En cualquier caso, si la atención a la mujer no lo requiere y no se recoge información personal, no hay tratamiento que realizar sujeto a la normativa de protección de datos.

Hay que tener en cuenta que la urgencia que pudiera requerir una atención inmediata no puede verse afectada por la necesidad de cumplimentar aspectos formales como el que nos ocupa; pero esto no significa que no deba cumplimentarse en un momento posterior.

Hay que concienciarse de que el objetivo de la normativa de protección de datos no es obstaculizar la atención de un colectivo sensible como el que nos ocupa sino garantizar la con-

fidencialidad y seguridad de una información personal. La información personal hay que tratarla con suma delicadeza para evitar que se participe esa información de forma no deseada e innecesaria a personas de la organización que no tienen por qué conocerla o que llegue a conocimiento del entorno del agresor y a conocimiento de éste.

A estos efectos la normativa de protección de datos se erige en una herramienta valiosa y operativa para garantizar la seguridad y confidencialidad que la persona requiere en un contexto de riesgo para su integridad física y/o emocional.

E) APLICACIÓN PARA DISPOSITIVOS MÓVILES

Y por último, si se optara por el diseño de una aplicación para dispositivos móviles que permitiera poner en contacto a mujeres que enfrentan violencia y a la Administración Pública, dicha aplicación debería incluir las cuestiones ya explicadas en cuanto a información y consentimiento, a cuyos efectos la Administración debe tener medios técnicos para acreditar que dicha información se ha explicado y que se ha recogido su consentimiento.

TERCERA CUESTIÓN:

¿QUÉ DATOS PUEDO SOLICITAR A UNA MUJER VÍCTIMA DE VIOLENCIA?

Otra pregunta que debe afrontar una persona que recoge datos de mujeres que han sido objeto de violencia es qué datos debe recoger y qué datos no debe recoger.

Los datos personales que se recojan deben ser los que requiera la actuación asistencial que necesite la persona. De modo que habrá que recoger el número de datos que sea necesario para llevar a cabo la atención que requiera la mujer. Ello no implica contar con formularios distintos sino que el personal técnico sepa en cada ocasión qué información debe completar, solicitando a la persona aquellos datos que estrictamente sean necesarios para ayudar a resolver el problema concreto que tiene.

Esta actuación, que constituye una atención correcta a las mujeres que enfrentan violencia, es asimismo un requisito legal en materia de protección de datos personales, debiendo limitarse la recogida de datos a aquellos que sean proporcionados, no excesivos, adecuados y pertinentes.

Además, en aquellos datos que se refieren a terceras personas habrá que tener especial cuidado, recogiendo los datos imprescindibles para la atención, como ocurre con los datos relativos a otros familiares, hijos, hijas o ascendientes, e incluso con los datos personales del propio agresor.

Es conveniente diseñar un formulario de recogida adaptado a las distintas opciones o finalidades que pueden tener aquellas administraciones que trabajan en la materia y facilitar así el trabajo. Asimismo, se debe generalizar una cláusula de información y recogida adaptada a las distintas posibilidades para informar y recoger el consentimiento en los distintos supuestos.

A tal propósito se dirige la cláusula de consentimiento informado para la recogida y cesión de datos personales de mujeres víctimas de violencia anteriormente mencionada y que se incluye, como anexo 1, en esta guía.

CUARTA CUESTIÓN:

¿CÓMO RECOJO LOS DATOS PERSONALES DE LA MUJER VÍCTIMA DE VIOLENCIA?

Esta cuestión suele ser pasada por alto, dando por sentado que se realizará adecuadamente. Sin embargo creemos conveniente dedicar algunas líneas a la forma en la que se recogen los datos. En este caso, hay varias preguntas a responder.

A) CONFIDENCIALIDAD EN LA RECOGIDA

La primera de ellas, es el contexto en el que se realiza la recogida. Se exige confidencialidad en el tratamiento de los datos personales, y ello exige también confidencialidad en la recogida. No se deben recoger datos personales de mujeres víctimas de violencia en salas comunes, salas compartidas con personal dedicado a otras cuestiones, o lugares que no permiten el debido aislamiento acústico. Las administraciones deben realizar un esfuerzo importante en esta cuestión.

Tampoco debe señalizarse con carteles una zona para la atención a este colectivo que permita la identificación visual de aquellas personas que necesitan esta ayuda, ni la ubicación de listas que identifiquen a las mujeres víctimas de violencia, por ejemplo, con una serie de citas horarias o similares. Siendo conscientes de que existe el riesgo de no localizar adecuadamente los puntos de atención, debe tenderse a formulaciones genéricas, de forma que, por ejemplo un panel indicativo a la entrada relacione las estancias con la actividad que desarrollan (Sala 1- violencia contra las mujeres) y que la estancia únicamente se identifique con su número de referencia. Otra posibilidad es que el servicio de información oriente en este sentido a las personas interesadas.

En definitiva, debe tratarse la atención a las mujeres víctimas de violencia con la debida confidencialidad, impidiendo que terceras personas puedan identificar como tales a determinadas personas. Y una vez iniciada la recogida de información, ésta se debe realizar en lugares cerrados con acceso restringido y proporcionando la debida intimidad.

B) GRABACIÓN DE AUDIO O VIDEO

Una cuestión relevante es la utilización de medios técnicos de grabación de audio o de imágenes para documentar la recogida de esta información. No existe impedimento legal alguno para que se acompañe a los sistemas de recogida de datos la grabación de audio y/o video de las sesiones de entrevistas con la mujer víctima de violencia. Sin embargo, sí que hay que hacer algunas matizaciones.

— La grabación debe realizarse con las condiciones adecuadas de seguridad y confidencialidad.

— Antes de proceder a la grabación, se debe constituir el fichero de imágenes y/o audio proveniente de las entrevistas, y declararlo e inscribirlo en el Registro correspondiente. No se trata de un fichero independiente del de violencia de género sino que en cada fichero de este tipo correspondiente a cada organismo deberá indicarse la "imagen y sonido" como tipo de dato recogido. Es muy importante significar que actualmente los ayuntamientos vascos carecen de ficheros de violencia de género inscritos, a pesar de ser una actuación básica. Su ausencia es inconcebible en todo tratamiento de datos personales pero muy especialmente en este tipo de datos a los que la normativa protege, por las razones expresadas, con el más alto grado de seguridad, tutela y cuidado.

— Antes de proceder a la grabación, la mujer víctima de violencia debe ser avisada convenientemente de ese extremo, indicando detalladamente qué se va a grabar, quién va a tener acceso a las grabaciones, qué finalidad tiene la grabación, cuándo se va a destruir y si se ha constituido un fichero expresamente para dichas imágenes o se van a guardar dentro del fichero de datos relacionados con mujeres víctimas de violencia.

— Una vez informada, habría que recoger su consentimiento para dicha grabación, incorporando a las cláusulas de recogida de información una mención específica sobre el consentimiento para la grabación.

— Se debe mantener en relación con las grabaciones las mismas medidas de seguridad y previsión de confidencialidad que para el resto de los datos de mujeres víctimas de violencia, y que en este caso es el nivel máximo previsto por la LOPD -nivel alto- y que veremos a continuación.

— Las grabaciones deben ser eliminadas en el plazo máximo de un mes. Cualquier utilización más allá de este periodo debe ser objeto de una valoración específica por parte del órgano responsable del servicio, acorde a la finalidad de la misma y a sus contenidos.

— Las grabaciones deben ser custodiadas y analizar detalladamente y de forma muy restrictiva las posibilidades de cesión o utilización al margen de la finalidad principal, que es documentar el proceso de recogida de información.

C) EN COMPAÑÍA DE QUIÉN

También es importante definir, en relación con el desarrollo de la recogida, si a la misma pueden acceder otras personas, como acompañantes, familiares u otras.

Es conveniente que en la entrevista, en la parte que se corresponde con la recogida de datos en sí misma, no participe nadie más que no sea la mujer víctima de violencia y la técnica o técnico que realiza la recogida. No obstante, esta consideración decaerá ante la prioridad de atender a otras necesidades de la persona como puede ser facilitar una comprensión adecuada de los términos de la conversación que requiera la intervención de otra persona (pensemos en personas con alguna minusvalía o discapacidad física o psíquica o dificultades para la comprensión del idioma, e incluso en situaciones de nerviosismo de la persona).

En todo caso, y si se verifica la recogida de datos en presencia de terceras personas, todo ello debe ser con la advertencia de la debida confidencialidad sobre los datos recogidos y dejando constancia en la recogida de dicha presencia.

D) DATOS DE TERCERAS PERSONAS

Una cuestión esencial a debatir en este apartado es la posibilidad de recoger datos de terceras personas facilitados por la mujer que enfrenta violencia. En principio, la posibilidad de recoger datos de terceras personas (familiares, ascendientes o descendientes, vecinos y vecinas o personas conocedoras de los hechos, o incluso el propio agresor) debe restringirse al máximo, recogiendo solo los datos estrictamente necesarios y con la indicación de tratarse de datos referidos -esto es, relativos a terceras personas- y respecto de los cuales no consta el consentimiento para la recogida.

En relación a los hijos e hijas menores de catorce años, no sería preciso adoptar ninguna medida, ya que el consentimiento lo suple la voluntad de alguno de los progenitores. Sin embargo, tratándose de hijos o de hijas mayores de catorce años y, por supuesto, mayores de dieciocho, es preciso seguir las mismas indicaciones que respecto de lo mencionado anteriormente sobre del tratamiento de datos de terceras personas.

Hay que señalar que la aplicación estricta del principio de calidad previsto en la ley orgánica de protección de datos exige la recogida de aquellos datos que sean pertinentes y, sobre todo, no excesivos para la finalidad para la que se recogen. Sin embargo, y teniendo en cuen-

ta la especial sensibilidad de este colectivo, sería aceptable una recogida de información ampliada, preventiva y previsora, con un signo protector y tutelar y dentro de los márgenes de la prudencia, ya que la atención integral de la víctima puede exigir disponer de más información sobre el contexto de la víctima que ayude a la elaboración de planes integrales de atención, o políticas de prevención de las víctimas de violencia.

Conforme a la normativa, recogidos los datos de terceras personas será preciso poner en conocimiento de aquéllas dicha recogida, así como el hecho de que los datos constan en el fichero en poder de la administración correspondiente. Sin embargo, hay que tener en cuenta el riesgo de exponer con tal comunicación la seguridad de la mujer, peligrando su integridad física o psíquica o el riesgo de exposición pública, circunstancias que son compatibles con la confidencialidad, de forma que habrá que priorizar su seguridad sobre la información para la preservación de valores superiores de la persona concurrentes como en este caso es la vida, y que con tan elevada consideración es recogido por la Declaración Universal de Derechos Humanos.

2. TRATAMIENTO DE DATOS PERSONALES

2. UNA VEZ RECOGIDOS LOS DATOS PERSONALES DE LAS VÍCTIMAS DE VIOLENCIA CONTRA LAS MUJERES, ¿QUÉ PUEDO HACER CON ELLOS? EL TRATAMIENTO DE LOS DATOS PERSONALES

PRIMERA CUESTIÓN:

¿TODO EL PERSONAL DE UN ORGANISMO DE ATENCIÓN A LA MUJER VÍCTIMA DE VIOLENCIA TIENE ACCESO A LOS DATOS PERSONALES?

Abordamos en este apartado las cuestiones relacionadas al tratamiento de los datos personales. Los requisitos que establece la ley para el tratamiento de los datos personales en parte ya han sido explicados previamente.

Tratamiento serán los distintos usos que se realicen de la información por la administración que los recoge, en este caso, y dependiendo de la administración hablaríamos de una finalidad asistencial, social, de otorgamiento de subvenciones, curativa, o de persecución del delito, entre otras.

La confidencialidad en el tratamiento es un requisito absolutamente imprescindible en todo caso y debe ser el principio más importante a seguir en la organización para impedir el acceso a los datos personales de personas, individuales o pertenecientes a organizaciones públicas o privadas, que no tienen ninguna necesidad de conocerlos para su actividad en la misma.

Así, es preciso realizar un proceso de reflexión y determinar quién en la organización necesita conocer los datos personales en el contexto de escenarios de violencia contra las mujeres para la finalidad de que se trate en cada supuesto.

Por lo tanto, como principio esencial en el tratamiento, los datos personales deben ser accesibles sólo a aquellas personas que necesariamente deben conocerlos por razón de su participación en el proceso de atención.

Se plantea habitualmente si estos datos se pueden poner en conocimiento de otras personas integrantes de la organización, como por ejemplo, de concejales y concejalas o de técnicos y técnicas que los demanden en el ámbito municipal; si se pueden comunicar a una o un superior jerárquico o a personas de otro servicio que los solicite.

La respuesta proviene del análisis concreto de cada supuesto, desde dos parámetros principales: el primero, analizar si hay alguna norma de rango legal que prevea esta cesión; si la

hubiera, dicha cesión puede realizarse sin ningún problema. El segundo, analizar si disponemos del consentimiento de la mujer para dicha cesión y en su caso recabarlo.

Hemos indicado que en los nuevos supuestos de recogida de datos de mujeres víctimas de violencia debemos incluir la previsión de las futuras cesiones, y así se recoge en la cláusula de consentimiento informado para la recogida y cesión de datos personales de mujeres víctimas de violencia que obra en el anexo 1 de esta guía, teniendo en cuenta que dicha previsión de cesión debe ser expresa y determinada, es decir, no puede ser genérica (del tipo de "las cesiones que se consideren necesarias...").

SEGUNDA CUESTIÓN:

¿PODEMOS DESTINAR LOS DATOS PERSONALES RECABADOS A OTRAS FINALIDADES DISTINTAS PARA LAS QUE SE RECOGIERON INICIALMENTE?

Como hemos visto, como principio esencial en el tratamiento, los datos personales deben guardarse sólo al alcance de aquellas personas que necesariamente deben conocerlos por razón de su participación en el proceso de atención a la mujer víctima de violencia.

Esto es, el tratamiento viene regido por el principio de calidad/finalidad.

En ningún caso, a salvo de algunas excepciones que veremos, se podrán destinar los datos a otras finalidades diferentes a aquéllas para las que se han recogido. Así pues, no es posible que los datos recogidos con una finalidad asistencial, acaben siendo utilizados para otro fin.

Esto tiene una explicación muy clara, y guarda relación con los requisitos de información y de consentimiento ya expresados, ya que no se puede consentir lo que no se conoce. Si hemos informado a una mujer víctima de violencia de que recogemos sus datos con una finalidad curativa, por ejemplo en el caso de un médico o médica, sea del sistema público o de una entidad privada, éste no podrá utilizar los datos más que para esta finalidad, y no para otras. No podrá por ejemplo, utilizarlos para ofrecerle productos o servicios comerciales de un laboratorio, ni destinarlos a otros fines, sean comerciales o no.

TERCERA CUESTIÓN:

¿CÓMO GARANTIZAMOS LA CONFIDENCIALIDAD DE DATOS PERSONALES EN PROCESOS DE CONCURRENCIA PÚBLICA?

El tratamiento de los datos debe respetar un evidente principio de confidencialidad, es decir, no podrán comentarse, debatirse o utilizarse de ningún modo, si no es para la mejora de la atención o la optimización de la atención que se va a prestar.

Hay que tener en cuenta también en el ámbito del tratamiento de los datos personales, las cuestiones derivadas de las convocatorias de ayudas dirigidas total o parcialmente a mujeres víctimas de violencia.

Tras un análisis de las distintas posibilidades que existen de ayudas en el panorama asistencial del País Vasco, como es la gestión de ayudas municipales por los ayuntamientos, concluimos que existen varias posibilidades de convocatorias y que requieren distinta solución:

1) En primer lugar, convocatorias de ayudas específicamente destinadas a mujeres víctimas de violencia.

2) En segundo lugar, convocatoria de ayudas generales en las que hay un turno específico para este colectivo dentro de la convocatoria, en las que si se resuelve que no procede otorgar ninguna ayuda, éstas, en tanto no concedidas, se trasladan a la convocatoria general, acreciéndola o incrementándola.

3) En tercer lugar, las convocatorias generales a las que se presentan en igualdad de condiciones mujeres víctimas de violencia, existiendo en el baremo una puntuación específica por el hecho de esta circunstancia (con sentencia firme, con denuncia, etc.).

4) En último lugar, las convocatorias generales a las que se presentan mujeres víctimas de violencia en igualdad de condiciones en relación con el resto, sin ninguna puntuación específica por ello.

En el primer caso, la publicidad de unas ayudas dirigidas exclusivamente a mujeres víctimas de violencia debe, en principio, ser restringida en cuanto a los datos que se facilitan a las personas interesadas que no son otras que las participantes en el proceso, y dirigida exclusivamente a las propias personas que participan en el proceso de otorgamiento de subvenciones.

Es importante en este caso que el resto de participantes en el proceso puedan conocer y acceder a la información sobre el resto de participantes, dado que se ven afectados sus derechos. Pero no la totalidad de la información; esto es, el derecho de acceso a esa información lo posee la persona interesada, entendiendo como tal aquélla que no ha obtenido la ayuda a

la que concurría en igualdad de condiciones con otras solicitantes y ese acceso, o conocimiento de la información, no lo es a toda la información sino sólo a la imprescindible para comprobar que la ayuda ha sido otorgada de forma objetiva a las personas beneficiarias.

Esta limitación, vinculada al principio de calidad en el tratamiento de datos personales, es respetuosa con el planteamiento y propósito que subyace en la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, en vigor a partir del 10 de diciembre de 2014, que pretende abrir a la ciudadanía el conocimiento de la información pública ante su demanda de unas administraciones diáfanas que comuniquen todo lo que hacen y en qué gastan los recursos económicos de la ciudadanía. Para ello prevé la publicidad activa de las administraciones públicas, así como sus planes, contratos públicos, convenios, subvenciones, presupuestos y retribuciones, entre otros datos, quedando esta información accesible a la ciudadanía.

Esta norma obligará a redefinir la actuación de la administración bajo el prisma de la protección de datos para evitar confundir transparencia con divulgación de información personal no exento de control sobre lo que se muestra.

En el segundo caso (cuando existe un turno específico para mujeres víctimas de violencia pero de no concederse la ayuda, estas mujeres pasan a la convocatoria general), se plantea el problema de si se afectan o no los derechos del resto de participantes en la convocatoria si se les da información relacionada con las mujeres víctimas de violencia que también se han presentado a la convocatoria. En este caso, hay que tener en cuenta que si las ayudas no concedidas en el turno de violencia acrecen a la convocatoria general éste es el elemento determinante, y el resto de participantes que no hayan obtenido la ayuda podrían tener acceso al expediente de las solicitantes en quienes, concurriendo la circunstancia de violencia, hubieran sido adjudicatarias, a los efectos de comprobar que cumple los requisitos de la convocatoria. ¿Ello conlleva conocer su identidad, domicilio, etc.? La respuesta debe ser negativa, debería tener acceso exclusivamente a los datos relacionados con el cumplimiento de las bases de la convocatoria; es decir, se debe conceder un acceso restringido.

En el tercero de los casos (convocatorias generales con una puntuación específica para las mujeres víctimas de violencia en la baremación), igualmente, el principio a aplicar en la respuesta, además de los principios generales de la protección de datos, es garantizar el derecho del resto de participantes en el proceso, que podrán verificar la circunstancia de mujer víctima de alguna de las participantes. En este caso, la identidad de las mujeres víctimas de violencia debe protegerse con carácter general. Se permitirá un acceso restringido al resto de solicitantes si así lo pidieran en defensa de sus intereses, sin acceso a la identidad de las solicitantes, sino simplemente a su circunstancia de mujer víctima de violencia en aras a acreditar el beneficio de la concesión de la ayuda al otorgarse una puntuación específica por esta circunstancia.

En el cuarto supuesto (convocatorias generales a las que acceden mujeres víctimas de violencia), no se plantea ningún problema en relación con la protección de datos, ya que en este casoal no tienen que acreditar su condición de mujer víctima de violencia. Si se recogiera ese dato sin haber necesidad de ello, se generaría un problema por el hecho de la propia recogida, al recabar un dato personal que es innecesario para el proceso.

Estas soluciones, en un planteamiento general, también son aplicables a las convocatorias de acceso a la función pública, convocatorias de bolsas de trabajo, etc. En éstas, cada persona podrá acceder a su propia información en el proceso, y también podrá acceder a la de los demás participantes cuando sea parte interesada al resultar perjudicada por la no obtención de la plaza convocada, así como mantenerse un acceso restringido de la información de las mujeres de violencia en los términos antes expuestos.

CUARTA CUESTIÓN:

¿PODRÍAMOS UTILIZAR LOS DATOS PERSONALES DE LAS MUJERES VÍCTIMAS DE VIOLENCIA PARA FINALIDADES ESTADÍSTICAS?

Una de las utilidades de la recopilación de datos personales es la realización de estadísticas para su posterior utilización en este contexto.

La respuesta inicialmente es sí, por cuanto la normativa de protección de datos permite que puedan ser usados para fines históricos, estadísticos o científicos, aunque no se recogiesen inicialmente con esta intención. Sin embargo, es necesario que para este propósito se anonimicen los datos personales, esto es que se eliminen los datos personales que permitan identificar o hacer identificable a una persona.

Debe, no obstante, llamarse la atención sobre la circunstancia de que la legislación vigente en materia estadística es la que determina qué utilización puede darse de los datos personales y qué finalidad preside el propósito estadístico. Esto es, si un ayuntamiento o Emakunde quieren efectuar estadísticas públicas deben hacerlo conforme a las exigencias impuestas por la legislación estadística, encontrándose actualmente en proceso de reforma Ley 4/1986, de 23 de abril, de Estadística de la Comunidad Autónoma de Euskadi.

Entre esas exigencias se encuentra la contenida en el artículo 9 de esta ley y que, como decimos, se encuentra en proceso de actualización. Dicho precepto señala que es el Plan Vasco de Estadística, de necesaria aprobación mediante una ley, el instrumento ordenador de la actividad estadística de la Comunidad Autónoma de Euskadi, y que el plan contendrá las estadísticas y otras actividades de esta naturaleza a realizar durante el periodo de su vigencia. Y exceptúa de la necesidad de declaración expresa la inclusión en dicho plan de todas las actividades estadísticas que sean objeto de convenios de cooperación entre el Estado y la Comunidad Autónoma de Euskadi.

Hay que señalar que la finalidad estadística es un uso de los datos personales que es necesariamente posterior a su recogida. Recogida cuya finalidad esencial es la atención de las mujeres que recaban atención y asesoramiento. Por lo tanto no podría incluirse en el contenido de la cláusula de consentimiento Informado una necesidad que no es consustancial al motivo por el cual la mujer ha acudido al servicio.

Por otra parte, hay que tener en cuenta que la recogida de datos personales con una finalidad estadística en el momento inicial es incompatible con un tratamiento anonimizado de datos personales en la práctica estadística. Dicho de otro modo, si la elaboración de estadísticas requiere la anonimización de los datos personales, no es correcto recabar los datos personales con una pretendida finalidad estadística puesto que ésta debe prescindir de esos datos.

3. CESIÓN DE DATOS PERSONALES

3. CÓMO COMUNICAR A TERCERAS PERSONAS LOS DATOS PERSONALES RELACIONADOS CON LA VIOLENCIA CONTRA LAS MUJERES. LA CESIÓN DE LOS DATOS PERSONALES

PRIMERA CUESTIÓN:

¿SE PUEDEN CEDER DATOS DE UNA MUJER VÍCTIMA DE VIOLENCIA A OTRAS PERSONAS O ENTIDADES?

En este caso, hemos detectado dos tipos de problemas. Por un lado, las comunicaciones de datos a personas de la misma organización (comunicación o participación de datos de un servicio de violencia a concejales o concejalas, por ejemplo) y, por otro, las cesiones entre distintas organizaciones (el ayuntamiento A recoge los datos y los cede a Osakidetza, a la asociación B, etc.).

Se plantea habitualmente si estos datos personales se pueden poner en conocimiento de otros personas integrantes de la organización (2), como por ejemplo, si se pueden poner en conocimiento de un concejal o concejala que los demande en el ámbito municipal, si se pueden comunicar a una o un superior jerárquico o a personas de otro servicio que los solicite, en cualquier administración.

La respuesta a esta pregunta debe venir del análisis concreto de cada supuesto, desde dos parámetros principales, que han sido expuestos más arriba y que reiteramos por su importancia: el primero, analizar si hay alguna norma de rango legal que prevea esta cesión; si la hubiera, dicha cesión puede realizarse sin ningún problema. El segundo, analizar si disponemos del consentimiento de la mujer víctima de violencia para dicha cesión, y en su caso recabarlo, requiriéndole para que autorice expresamente la cesión.

Ya hemos indicado que en recogida de datos es conveniente prever las futuras cesiones, conforme consta en la cláusula de consentimiento informado para la recogida y la cesión de datos personales de mujeres víctimas de violencia obrante al anexo 1 de esta guía. Dicha previsión de cesión debe ser expresa y determinada (a qué instituciones en concreto), es decir, no puede ser genérica (del tipo de "las cesiones que se consideren necesarias…").

(2) Aclarar que, dentro de la organización, la comunicación de datos personales no es una cesión siempre que se produzca entre personas autorizadas para tener conocimiento de esa información.

SEGUNDA CUESTIÓN:

¿ES POSIBLE LA CESIÓN DE DATOS PERSONALES ENTRE PERSONAS O ENTIDADES QUE INTEGRAN UN PROTOCOLO DE COLABORACIÓN PARA LA ATENCIÓN INTEGRAL A MUJERES VÍCTIMAS DE VIOLENCIA?

Se están desarrollando estos últimos años en distintos municipios del País Vasco los denominados "protocolos" de atención a mujeres víctimas de violencia que buscan establecer un marco de colaboración entre las distintas instituciones de atención a este colectivo. En el ámbito municipal, principalmente la administración sanitaria, la administración municipal del ámbito de los servicios sociales, la administración policial, la fiscalía, o el poder judicial, así como algunas otras instituciones.

Estos protocolos siguen los principios establecidos en la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género así como en la Ley 4/2005 para la Igualdad de Mujeres y Hombres, que establece que se deberá promover la colaboración interinstitucional entre las distintas administraciones participantes en el proceso de atención. Sin embargo, exige una reflexión sobre las cesiones de datos que se pueden producir entre dichas administraciones.

Estas cesiones, al igual que hemos explicado anteriormente, deben estar previstas en una norma de rango legal (3) o, en su caso, deben realizarse con el consentimiento previo y expreso de la mujer víctima de violencia, que debe conocer qué cesiones concretas se van a realizar. También hay que tener claro como premisa que un protocolo firmado por varias instituciones no es suficiente amparo jurídico, por cuanto no es una norma de rango legal, para las cesiones que se produzcan al amparo del mismo. Por ello, es preciso recabar el consentimiento de la mujer para dichas cesiones dado el especial rigor y sensibilidad de este ámbito.

Además del consentimiento y de la habilitación expresa para la cesión de datos personales por una norma con rango legal, hay que señalar que existe una tercera posibilidad habilitante

(3) Actualmente no existe ninguna norma con rango legal habilitante específicamente dirigida a regular la cesión en materia de violencia, lo cual no obsta para que en cualquier momento se pueda producir una modificación legal o una nueva norma que lo incluya en el ámbito de la regulación de cualquiera de las instituciones intervinientes en este ámbito, sea estatal o autonómico. Al estudio de estas posibilidades se dirige el Informe preliminar de evaluación en materia de protección de datos personales del II Acuerdo Interinstitucional para la Mejora en la Atención a Mujeres Víctimas de Maltrato en el Ámbito Doméstico y de Violencia Sexual sobre adaptación a la normativa de protección de datos personales, que establece vías de solución para abordar adecuadamente la cesión de datos personales. En el momento actual no existen resquicios legales para salvar este escenario ni sería aconsejable que los hubiera en atención a una adecuada protección de los datos personales y de la propia mujer. La mentalización y concienciación en este punto es esencial y lo exige expresamente la ley.

de la cesión, y es que ésta se produzca entre órganos que posean las mismas competencias. Ello llevaría a validar la cesión de datos que se produce entre servicios sociales de distintos municipios, entre servicios sociales de un municipio y la diputación foral, o entre estos y el Gobierno Vasco, si bien esta posibilidad no es extensible a todos los integrantes de un protocolo de coordinación de atención social sino sólo a los que tienen competencias específicas en materia de servicios sociales.

El dictamen de la Agencia Vasca de Protección de Datos (AVPD) de 9/8/10 resuelve esta cuestión y concluye que se adecúa a la normativa de protección de datos personales de las cesiones en materia de servicios sociales cuando se producen entre órganos que posean las mismas competencias o competencias que versen sobre las mismas materias.

En este sentido, el dictamen de la AVPD señala que la atención de los servicios sociales son una materia en la que existe un ejercicio competencial compartido entre diferentes administraciones públicas vascas, siendo por ello de aplicación a las cesiones de datos que en este ámbito se produzca la excepción a la necesidad de consentimiento para la cesión de datos precedentemente señalada -mismas competencias o competencias sobre la misma materia-.

Esta posibilidad de compartir información está en consonancia con la obligación de coordinación recogida en la Ley 12/2008 de 5 de diciembre, de Servicios Sociales, que señala que las administraciones públicas vascas actuarán de conformidad con el deber de cooperación y coordinación entre sí, necesarias para garantizar la máxima coherencia, unidad, eficacia y eficiencia en el funcionamiento del sistema.

No obstante, y a pesar de que existe habilitación legal para compartir información en estos supuestos, hay que advertir también de la necesidad de tener en cuenta un principio básico en materia de protección de datos, como es el de calidad.

Conforme a este principio, los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Por lo tanto, y en aplicación de este principio, únicamente podrán ser objeto de cesión aquellos datos personales que cumplan dos condiciones:

1) Que ambos órganos, cedente y cesionario, ostenten mismas competencias o competencias que versen sobre las mismas materias, y

2) Que los datos objeto de cesión se limiten únicamente a los datos adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

De ese modo, ante peticiones de datos personales de otras instituciones, participen o no en el protocolo municipal de colaboración, la reacción debe ser en todo caso la expuesta: primero, analizar si hay norma de rango legal habilitante que permita expresamente la cesión o que la comunicación se pretenda entre distintos órganos con las mismas competencias, ambos, que se dirijan a atender la misma finalidad; esto es, entre órganos con las mismas competencias o competencias sobre las mismas materias; y segundo, si no lo hubiera, analizar si se cuenta con el consentimiento de la mujer víctima de violencia o recabarlo expresamente. Si no se da alguno de estos parámetros, la cesión no debe producirse.

En todo caso, y de cara al futuro, se deberá recoger, como pauta general, el consentimiento de la mujer víctima de violencia para las cesiones concretas futuras que se hagan, conforme a la cláusula de consentimiento informado para la recogida y cesión de datos personales de mujeres víctimas de violencia obrante al anexo 1, incluyendo en dicha recogida los cesionarios concretos que van a recibir dichos datos (4).

Durante el tratamiento de los datos personales la única persona que sí va a poder acceder a sus datos personales, conocer cuáles datos obran en poder de la administración, rectificar dichos datos personales si son incorrectos, oponerse a su tratamiento o solicitar su cancelación, será la propia mujer en el ejercicio de sus derechos ARCO (derechos de acceso, rectificación, cancelación y oposición al tratamiento de los datos personales propios).

TERCERA CUESTIÓN:

¿SE PUEDEN CEDER A LOS SERVICIOS SOCIALES, O ENTRE DISTINTAS ÁREAS DE SERVICIOS SOCIALES, DATOS PERSONALES DE UNA PERSONA MENOR DE EDAD QUE VIVA EN UNA SUPUESTA SITUACIÓN DE VIOLENCIA?

Dada la relevancia intrínseca de esta cuestión se ha expuesto el planteamiento íntegro en el anexo 3, indicándose aquí las consideraciones que han determinado su análisis jurídico.

Tal y como se ha venido indicando, las cesiones tienen como regla general el consentimiento, y ésta ha sido, y debe ser, la recomendación más importante en la materia. Sin embargo, como también hemos indicado, es posible que las cesiones de datos tengan una habilitación legal, es decir, haya una norma de rango legal que habilite la cesión. Dicha norma

(4) Al menos mientras no exista una norma legal habilitante de la cesión en el ámbito de los servicios sociales que pudiera venir dada por la reforma de la Ley Orgánica 1/2004, o por su regulación en una futura ley municipal.

debe ser expresa, y no genérica, y supone un análisis de su redacción para poder concluir si en efecto es o no título suficiente.

Analizado el panorama jurídico operante en esta materia, cuya valoración consta en el anexo 3, se concluye en que es un título legal habilitante para la cesión de datos de menores en situación de desamparo la previsión del artículo 58.1 de la Ley 3/2005 del 18 de febrero de Atención y Protección a la Infancia y la Adolescencia, con los siguientes límites: primero, afecta sólo a supuestos de desamparo y a partir de que la administración conozca esta situación; segundo, no habilita a la cesión de expedientes íntegros, sino a la elaboración de informes que, puntualmente y sólo en la medida en que sea imprescindible, pueden contener datos o informaciones en poder de otras administraciones públicas; tercero, debe tenerse en cuenta en todo momento la aplicación del principio de calidad, especialmente recogido en el propio artículo 58.1, que indica que sólo se podrán ceder aquellos datos estrictamente necesarios para la finalidad perseguida y, por lo tanto, a órganos con competencia en la materia que, en este caso, es el servicio que se determine para atender a las personas menores de edad.

CUARTA CUESTIÓN:

¿PUEDE FACILITARSE INFORMACIÓN DE CARÁCTER PERSONAL POR VÍA TELEFÓNICA?

Por último, en este capítulo, procede realizar una mención a los sistemas de atención telefónica a la ciudadanía. A este respecto, no es posible facilitar información a una persona que se dirige por teléfono a la administración en ningún caso sin una certeza razonable de que es quien dice ser. Pero especialmente se debe restringir la entrega de información a personas que se dirijan por teléfono a la organización sin dicha comprobación cuando se trata de datos de nivel alto equivalentes a datos especialmente protegidos.

La comprobación de identidad puede atenerse a diversos sistemas, como facilitar un número de expediente a la persona al inicio del procedimiento administrativo y requerir dicho número junto con alguna otra pregunta de comprobación de identidad, de forma que todas ellas combinadas aseguren la identidad de la persona.

Ante cualquier duda, la información no debe ser facilitada a la persona que se dirige por teléfono, requiriéndole para que acuda presencialmente. Otra opción válida es responder a preguntas en las que el operador u operadora indique sí o no a informaciones que la persona comunicante ya conoce, sin extenderse en la respuesta y sin facilitar ninguna información añadida.

4. SEGURIDAD DE DATOS PERSONALES

4. LA SEGURIDAD DE LOS DATOS PERSONALES: CÓMO DEBEMOS CUSTODIAR LOS DATOS DE LAS MUJERES VÍCTIMAS DE LA VIOLENCIA

La Ley Orgánica de Protección de Datos de Carácter Personal no incluyó entre los datos especialmente protegidos los datos provenientes o relacionados con las mujeres víctimas de violencia. Esto habría otorgado el status de datos con un mayor nivel de protección a este tipo de datos personales. Sin embargo, el Reglamento 1720/2007 que desarrolla la LOPD incluye una importante mención que en la práctica supone que los datos relacionados con la violencia de género adquieran este nivel de protección (5). Ello fue el otorgar a este tipo de datos la obligación de ser protegidos con medidas de seguridad de nivel alto.

PRIMERA CUESTIÓN:

¿CUÁLES SON LAS PRECAUCIONES O MEDIDAS DE SEGURIDAD QUE HAY QUE ADOPTAR EN RELACIÓN CON LOS DATOS PERSONALES DE LAS MUJERES VÍCTIMAS DE VIOLENCIA?

Las medidas de seguridad se aplican en tres niveles de seguridad; las medidas de nivel básico, de nivel medio y de nivel alto. Estas medidas de seguridad se establecen con detalle en el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal y se deben aplicar de una forma acumulativa, es decir, que deben aplicarse las medidas de nivel básico a todo tipo de datos; a los datos de nivel medio se aplicarán las medidas de nivel básico y las de nivel medio y, a los datos de nivel alto se aplicarán las medidas de nivel básico, medio y alto.

Por lo tanto, a los datos personales derivados de actos de violencia de género se aplicarán todas las medidas de seguridad; esto es, las de nivel básico, más las de nivel medio, más las de nivel alto. Se trata de obligaciones legales que aluden a contenidos mínimos de exigido cumplimiento, y cuyo incumplimiento o inadecuado cumplimiento determina la imposición de sanciones o declaración de infracción por las instituciones de control en materia de protección de datos.

De una forma resumida, las medidas aplicables a los ficheros de datos provenientes de una mujer víctima de violencia serían las siguientes:

---

(5) Nos remitimos a las precisiones en relación al concepto "violencia contra las mujeres" contenidas en las páginas 16 y 17 de la presente guía.

— La primera y más importante, es dotarse de un documento de seguridad actualizado. Se trata de una medida de seguridad básica y es el documento que define las funciones y obligaciones del personal, así como las implicaciones en que el personal pudiera incurrir en caso de incumplimiento.

  Se trata de un documento interno de la organización, que debe mantenerse siempre actualizado. Disponer del documento de seguridad es una obligación con independencia del nivel de seguridad que sea necesario aplicar.

  Los apartados mínimos que debe incluir el documento de seguridad son los siguientes:

  - Ámbito de aplicación: especificación detallada de los recursos protegidos.
  - Medidas, normas, procedimientos, reglas y estándares de seguridad.
  - Funciones y obligaciones del personal.
  - Estructura y descripción de los ficheros y sistemas de información.
  - Procedimiento de notificación, gestión y respuesta ante incidencias.
  - Procedimiento de copias de respaldo y recuperación de datos.
  - Medidas adoptadas en el transporte, destrucción y/o reutilización de soportes y documentos.

— Una vez que contemos con el documento de seguridad, es preciso que la organización lo conozca, lo interiorice y adopte las medidas que en él se exponen en su quehacer diario. Para ello, la formación continua y la sensibilización de las personas se convierte en fundamental.

— Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro.

— Una incidencia es todo suceso que puede comprometer alguno de los aspectos relacionados con la seguridad de la información confidencialidad, integridad y disponibilidad- por fugas, pérdida de la información o sustracción; en definitiva, por actuaciones involuntarias o intencionadas.

— Un procedimiento de notificación de incidencias exige establecer unas reglas para que todo el personal gestione correctamente los incidentes y se minimice el impacto derivado de éste, para lo cual debe contarse con un procedimiento conocido por todo el personal que trate datos de carácter personal, y que permita la comunicación, registro y documentación, seguimiento, respuesta y cierre de los incidentes.

— Las personas usuarias tendrán acceso únicamente a aquellos recursos -esto es, medios o herramientas- que precisen para el desarrollo de sus funciones y será el o la responsable del fichero quien deberá encargarse de que exista una relación actualizada de personas usuarias y perfiles de usuarios y usuarias, y los accesos autorizados para cada una de esas personas usuarias.

— Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

— La salida de dichos soportes y documentos, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales deberá ser autorizada por el o la responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

— La entidad u órgano responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de las personas usuarias.

— La identificación es la actuación que permite al sistema reconocer a la persona usuaria; y la autenticación es la verificación que realiza el sistema sobre esta identificación, constituyendo el primer paso para garantizar el acceso únicamente de personas autorizadas.

  El medio habitual de autenticación en los procesos informáticos es la utilización de contraseñas, que deben asignarse, distribuirse y almacenarse de forma que se garantice su confidencialidad e integridad, no teniendo que divulgarse entre los trabajadores y las trabajadoras. Además, las contraseñas deben modificarse periódicamente y almacenarse de forma ininteligible.

— Deberán establecerse procedimientos de actuación para la realización, como mínimo semanal, de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

— A partir del nivel medio de seguridad, en el Documento de Seguridad deberán designarse una o varias personas responsables de seguridad encargadas de coordinar y controlar las medidas definidas en el mismo, como hemos indicado precedentemente al describir la naturaleza del documento de seguridad, debiendo efectuarse un control periódico del contenido del documento.

— Los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una Auditoría LOPD que verifique el cumplimiento de las medidas de seguridad en el tratamiento de datos de carácter personal. Además, deberá realizarse dicha auditoría siempre que se realicen modificaciones sustan-

ciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas; con la realización de esta auditoría de carácter extraordinario en los casos en los que proceda por haberse producido esa modificación sustancial queda iniciado el cómputo de dos años ordinarios.

— Deberá establecerse, además del sistema de registro de salida establecido como medida básica, un sistema de registro de entrada de soportes.

— Las salidas y entradas de soportes -documentos en papel o dispositivos tecnológicos- que contengan información personal serán anotadas, conforme a un procedimiento manual o informático. Se indicará, en las entradas: el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la recepción; y en el caso de las salidas: el tipo de documento o soporte, la fecha y hora, el o la destinataria, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la entrega.

— La entidad u órgano responsable del fichero o tratamiento establecerá un mecanismo para limitar la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

— A partir del nivel alto, exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

— La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte. Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando estos se encuentren fuera de las instalaciones que están bajo el control de la persona responsable del fichero. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado.

— Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan.

— De cada intento de acceso deberá guardarse información, como mínimo, la identificación del usuario o usuaria, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado,

será preciso guardar la información que permita identificar el registro al que se ha accedido.

— Además de estas cuestiones, y en relación a los ficheros no automatizados, es decir, aquellos que se tratan en papel, es importante indicar que los armarios, archivadores u otros elementos en los que se almacenen deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

— También hay que adoptar, en el caso de tratamiento de datos en papel, medidas de control del acceso de terceras persona, medidas de restricción de la realización de copias, así como control de las medidas relativas al traslado físico de la documentación.

De forma resumida, existen medidas de seguridad físicas (como es adaptar espacios) y medidas de seguridad técnicas que afectan a los sistemas de tratamiento. Asimismo, algunas medidas afectan a la organización del trabajo y a la forma de tratar los datos, y otras son puramente informáticas. Lo que es conveniente es adoptar un enfoque global de la seguridad, que permita un cumplimiento íntegro de la ley, así como un tratamiento correcto de los datos de las mujeres víctimas de violencia.

Contar con un desarrollo o sistema informático de verificación de la información personal no es el remedio que permita despreocuparse de un atento cumplimiento y adecuado tratamiento de los datos de carácter personal en la confianza de que el sistema informático tendrá en cuenta estos parámetros. Porque un sistema informático obedece a criterios técnicos basados en la operatividad, funcionalidad y rendimiento, y no en criterios jurídicos o legales cuyo conocimiento no es presupuesto necesario para su elaboración. Además, porque los dispositivos informáticos no son infalibles al comportamiento humano, intencionado o involuntario.

Las obligaciones que impone la normativa de protección de datos requieren también la cumplimentación de medidas de seguridad no informáticas y de la realización de actividades no informáticas: una correcta inscripción de ficheros y elaboración del necesario documento de seguridad, la redacción de contratos de encargo de tratamiento de datos personales -en la concesión de determinados servicios administrativos que requieran la utilización de datos personales-, una verificación -siquiera mínima- de cumplimiento de las medidas de seguridad exigidas por la normativa de protección de datos, la elaboración de una adecuada política de privacidad en las website, o la verificación del correcto tratamiento de la información personal. Además, es necesaria la información y formación del personal para conocer aspectos básicos como la forma de cumplimentar y procesar una solicitud de derecho ARCO, entre otras obligaciones.

Es por ello que no puede abandonarse en un programa o asistencia informática la verificación de los sistemas de información sino que es necesario conjuntar ambos aspectos: la funcionalidad del sistema y su seguridad en términos de protección de la información.

SEGUNDA CUESTIÓN:

¿TENGO QUE ADOPTAR MEDIDAS ESPECÍFICAS DE SEGURIDAD DEPENDIENDO DEL MEDIO POR EL QUE HAN LLEGADO LOS DATOS PERSONALES?

Tal y como hemos explicado anteriormente, hay varias formas para que los datos personales de una mujer víctima de violencia lleguen a la administración; a priori podemos pensar en la comunicación telefónica, la presencial, la utilización de la página web, el correo electrónico o mediante aplicaciones móviles. En todos ellos se debe garantizar mediante los procedimientos técnicos adecuados que una vez que los datos se encuentren en poder de la administración, estos se mantengan con las medidas de seguridad adecuadas expuestas anteriormente, y a disposición sólo de las personas que van a tratarlos.

El medio de comunicación, por lo tanto, será irrelevante a estos efectos, debiendo aplicar las mismas medidas y el principio de confidencialidad en todo caso; pero sí habrá que diseñar un sistema interno de gestión que garantice que sólo tendrán acceso a esos datos las personas que necesariamente deban tenerlo por razón de las tareas que tienen en la organización, descartando de dicho proceso a personas intermediarias o auxiliares que no tengan ningún motivo para el acceso a dichos datos.

En el caso de un servicio en el que participen varias personas, todas ellas podrán acceder a los datos personales de la mujer, siempre que dichas personas tengan un motivo para ello en el proceso administrativo; esto es, por aplicación de un principio esencial de la normativa sobre protección de datos, que es el principio de calidad, vinculado a la finalidad que es la de atenderle, asesorarle y ayudarle en las distintas soluciones de que puede disponer.

Dentro de esa finalidad, en el servicio administrativo de que se trata, hay una serie de mecanismos de funcionamiento que pueden exigir la revisión de recogida de información o de las resoluciones por la jefatura de servicio, o que pueden exigir por el reparto de tareas que un técnico o una técnica se encargue de la recogida de información y otra persona del tratamiento de la misma. Mientras se mantenga la finalidad en el tratamiento, esto no plantea problemas.

El problema surge cuando se cambia la finalidad, y se ceden los datos a otro servicio municipal que tiene otra finalidad distinta, por ejemplo, se ceden al servicio del padrón para verificar el domicilio y los convivientes, o a recaudación para otras verificaciones, o se ceden al concejal o concejala o al alcalde o alcaldesa.

Estas cesiones que se salen de la finalidad original, que es la amparada por el consentimiento inicial, en principio no pueden hacerse. Hay que tener en cuenta que la normativa vigente exige, para los datos relacionados con violencia contra las mujeres, medidas de seguridad de nivel alto, que son muy exigentes y no permiten, por ejemplo, entre otras muchas cuestiones, los accesos no autorizados, debiendo dejar huella de toda persona que accede al expediente, incluso los accesos autorizados.

TERCERA CUESTIÓN:

¿ES POSIBLE LA ELABORACIÓN POR EL PERSONAL DE FICHEROS PARALELOS A LAS BASES DE DATOS CORPORATIVAS PARA UN MEJOR MANEJO DE LOS DATOS PERSONALES DE LAS MUJERES VÍCTIMAS DE VIOLENCIA?

En ocasiones el personal técnico que realiza atención a mujeres víctimas de violencia incorpora los datos que recoge, además de a la base de datos corporativa, a otra base de datos creada paralelamente y que manejan sin supervisión de la o el responsable del tratamiento. Este tratamiento se realiza con una finalidad de disponer en todo momento de la información para conseguir una mejor atención a la mujer, pero sin embargo, produce importantes problemas de seguridad, ya que estos ficheros paralelos no están declarados a la Agencia de Protección de Datos competente ni sometidos a los requisitos de seguridad que establece la normativa.

La declaración del fichero ante la Agencia de Protección de Datos competente determina quién tiene el control y la responsabilidad de los datos que allí se contienen, quién decide en general sobre dichos datos. No es posible por lo tanto generar ficheros paralelos sobre los que la organización o entidad responsable del fichero no ejerza esta capacidad de control. En todo caso, si la organización en tanto responsable del tratamiento autorizara que se generaran almacenamientos paralelos o ficheros en otros formatos para facilitar su tratamiento, ello debería estar previsto en el documento de seguridad, para evitar problemas de fugas de información de seguridad en general.

Hay que señalar que la creación de estos ficheros temporales, o copias de trabajo y su mantenimiento, debe estar autorizada por las organizaciones o entidades responsables del fichero correspondiente. Esos ficheros deberán cumplir con el nivel de seguridad que les corresponda en función de la tipología de datos personales objeto de tratamiento y de la finalidad. Además, las organizaciones, en su cualidad de responsables del fichero, deberán dar la directriz por la que todo fichero temporal o copia de trabajo creado sea borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

Así pues, debe existir para tal caso una decisión de la organización para que la gestión de los datos se haga de una determinada forma, sin que haya lugar a la improvisación, y supervisando que no existan sistemas de acumulación de datos paralelos y desconocidos para la organización en tanto responsable del fichero, lo que podría provocar problemas de fugas de información.

CUARTA CUESTIÓN:

¿CUÁL ES EL USO RAZONABLE DE LOS SISTEMAS DE INFORMACIÓN POR EL PERSONAL QUE INTERVIENE EN LOS PROCESOS DE ATENCIÓN?

La normativa de protección de datos es de inexcusable observancia, siendo actualmente un ámbito de habitual demanda de la ciudadanía y de notoria repercusión en los medios de comunicación.

Las y los profesionales deben respetar esta normativa en el ejercicio de sus funciones, y además deben recibir formación periódica para su oportuno reciclaje en una materia en constante desarrollo y evolución como es la normativa sectorial de protección de datos, que tiene incidencia en otros aspectos normativos y, a la inversa, se ve influida por estos; a modo de ejemplo recordemos la ley de transparencia a que se ha hecho referencia más arriba o el futurible reglamento europeo, en fase final de aprobación por el Parlamento Europeo. Esta actualización periódica es imprescindible al objeto de realizar un uso adecuado en el manejo y tratamiento cotidiano de la información personal, y mantener un comportamiento respetuoso con la información personal de las personas usuarias del servicio, así como evitar afectación a los derechos de las personas que implique incurrir en diversas formas de responsabilidad.

A) LA RESPONSABILIDAD

La responsabilidad no es un aspecto desdeñable. Hay que tener en cuenta que si bien la normativa de protección de datos actual sólo contempla la imposición de sanciones económicas a profesionales u organizaciones del sector privado, por importes de 900 a 600.000 euros, en el caso de que la vulneración provenga de un órgano público no se impone sanción económica sino que se produce una declaración de infracción que, en todo caso, la administración deberá corregir.

No obstante, hay que advertir, por un lado, que el futuro reglamento europeo puede fijar sanciones económicas también en el ámbito de las administraciones públicas. Y, por otro lado, hay que anotar que una declaración de infracción emanada de las autoridades de control en protección de datos personales, puede determinar la apertura de un procedimiento disci-

plinario contra empleadas y empleados públicos individualmente considerados. (artículo 46.2 LOPD).

Además, existe una segunda vía a través de la cual la persona puede obtener una declaración de responsabilidad patrimonial de las administraciones públicas y la materialización de una indemnización económica. Se trata de la fijación de responsabilidad patrimonial por erróneo funcionamiento del servicio que puede derivar en la atribución de responsabilidad al funcionario o funcionaria en quien se personalice haber efectuado un tratamiento ilegítimo o inadecuado de la información personal, hasta el punto de poder exigirle participación en el abono de la indemnización que pudiera establecerse en vía administrativa o por un tribunal.

Esta posibilidad se encuentra expresamente regulada en el artículo 145.2 de la Ley 30/92 LRJPAC -Ley de Régimen Jurídico de las Administraciones Públicas y de Procedimiento Administrativo Común- que es el que habilita la apertura de procedimiento disciplinario al señalar que la administración correspondiente, cuando hubiere indemnizado a las personas lesionadas, exigirá de oficio de sus autoridades y demás personal a su servicio la responsabilidad en que hubieran incurrido por dolo, o culpa o negligencia graves.

Por todo ello, la formación del personal, directivo y empleado, es esencial en esta materia como forma de concienciación y de adopción de buenas prácticas en el tratamiento de la información de carácter personal y en la contención del riesgo de posibles responsabilidades derivadas de un inadecuado tratamiento que, incluso, puede derivar en la apertura de un proceso penal por delito de revelación de secretos de los artículos 197 y siguientes del Código Penal.

B) PROTOCOLO DE USO RAZONABLE DE RECURSOS

A continuación se expone un PROTOCOLO DE USO RAZONABLE DE RECURSOS por el personal a modo de aproximación a las actitudes básicas a desarrollar. Hay que advertir que este protocolo se limita a recoger las prácticas más elementales de utilización de medios corporativos y que es el primer y más básico estadio en la formación que requiere el desarrollo de la actividad que se analiza.

1. Adoptar actitudes tales como utilizar los mecanismos de cerradura para el almacenamiento de archivos de información (cajones, armarios, y puertas de despachos).

2. Identificar las carpetas manuales mediante códigos o expresiones cifradas.

3. Comprobar que no quedan documentos impresos que contengan información personal en la bandeja de salida de la impresora, ni en sitios o dependencias accesibles al público (mostrador, mesas donde se realicen reuniones o se reciban visitas).

4. Utilizar la destructora de papel y no reutilizar papel que contenga datos personales.

5. Política de mesas limpias. Dejar libre de documentación el puesto de trabajo al abandonarlo en descansos, pausas o fin de la jornada laboral, usando al efecto bien las cajoneras, bien los archivadores, debidamente cerrados.

6. Impedir la visualización del contenido de las pantallas.

7. Evitar ofrecer o solicitar información personal en la atención telefónica, procurando derivar la solicitud de dicha información a las citas con los trabajadores y trabajadoras que prestan la atención.

8. Cerrar o bloquear la sesión al término de la jornada laboral y al ausentarse temporalmente del puesto de trabajo.

9. No copiar, ni extraer de las oficinas, la información contenida en el sistema de información en el que se almacenan datos de carácter personal en cualquier soporte (papel o informático), sin autorización expresa del responsable del fichero.

10. Utilizar la contraseña propia, no intercambiarse o facilitarse la clave con compañeras y compañeros, y cambiarla con la periodicidad requerida por el sistema.

11. Comunicar a la persona responsable de seguridad las incidencias de seguridad de las que se tenga conocimiento.

12. Adoptar prácticas de uso responsable de Internet en orden a evitar el acceso a páginas no seguras que pueden afectar a los sistemas de información y a la información misma.

13. No remitir datos personales por correo electrónico salvo que estén autorizados. Además, para el envío de información de datos relacionados con la violencia contra las mujeres y datos de carácter personal de nivel alto -aquellos que incluyan datos relativos a la ideología, religión, creencias, origen racial, salud o vida sexual de las personas-, será imprescindible que el envío se realice adoptando necesariamente mecanismos que eviten que la información sea inteligible o manipulada por terceras personas (encriptación).

14. Si se envían correos electrónicos a más de un destinatario o destinataria debe utilizarse el sistema de copia oculta (CCO), evitando que cada persona pueda tener acceso a las direcciones del resto de partes de la comunicación.

No entra en esta consideración el envío de emails a las direcciones de correo electrónico que puedan ser conocidas por personal de las distintas áreas, toda vez que la revelación de dichas direcciones electrónicas corporativas se realiza con una finalidad de gestión y desarrollo de la actividad propia de la organización, cuyo ámbito es interno, cuando el conocimiento del personal es preciso y necesario. En suma, en este caso de ámbito interno, la utilización de copia oculta no sería necesaria siempre que no fuesen incorporadas direcciones personales de las trabajadoras y los trabajadores.

5. PERIODO DE CONSERVACIÓN O UTILIZACIÓN DE DATOS PERSONALES

5. UNA VEZ QUE SE HAN UTILIZADO LOS DATOS PERSONALES DE MUJERES VÍCTIMAS DE VIOLENCIA, ¿HASTA CUÁNDO SE PUEDE GUARDAR O UTILIZAR SUS DATOS PERSONALES?

¿Es acorde a la ley un mantenimiento "indefinido" de los datos personales en el fichero en poder de la institución correspondiente? Lo primero que hay que indicar para resolver esta cuestión es recordar lo ya expuesto en cuanto a la posibilidad de recoger y tratar datos de mujeres víctimas de violencia: sólo se podrán recoger y tratar aquellos datos relacionados directamente con la finalidad para la que se han recogido, no pudiendo cambiarse dicha finalidad.

De ese modo, los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquéllas para las que los datos hubieran sido recogidos.

Por lo tanto, es muy importante que se realice dicha reflexión en un momento inicial, para que el proceso de tratamiento sea correcto y vincular el mantenimiento de los datos personales al principio de finalidad. De ese modo, los datos personales deben cancelarse cuando hayan dejado de ser necesarios para la finalidad para la que fueron recabados.

La respuesta viene dada por la aplicación de este principio de finalidad, y por lo tanto, podrán mantenerse los datos personales de la mujer víctima de violencia en poder de la institución que los recogió siempre y cuando se mantenga la finalidad para la que se recogieron. La determinación del tiempo de atención que requiere una mujer en estas circunstancias debe ser objeto de determinación por el organismo, y finalizado este período procederá la cancelación de los datos. Igualmente, si hay una disposición de rango legal que obligue al mantenimiento del fichero con carácter indefinido, los datos personales que allí consten deberán guardarse de tal forma.

Esto es, respetando el propósito de no cronificar, es necesario diferenciar la situación de la persona que requiere una atención más prolongada en el tiempo o una intervención regular, de aquella otra persona que requiere una atención puntual, bien sea porque ha resuelto el problema, bien sea porque desea abandonar la atención, o bien porque traslada su residencia a otro lugar sobre el cual la organización no posee competencia. En todos estos casos, una vez agotada la finalidad de la atención, se deberán cancelar los datos de las personas beneficiarias. Para los casos en los que se necesite una atención permanente o extendida en el tiempo hay que valorar si es necesario mantener los datos durante un periodo de tiempo más largo.

Puede también ocurrir que se convoquen ayudas para mujeres víctimas de violencia, ayudas que tienen una duración determinada en el tiempo, porque se realice, por ejemplo, una convocatoria única al año: hay un periodo de presentación de solicitudes, un periodo de valoración y se comunica a las beneficiarias la concesión o denegación. En este caso, una vez agotada la finalidad de la convocatoria, que es la propia concesión, y si no existen facultades expresas de revisión de dicha convocatoria, se deberán cancelar los datos de las beneficiarias.

Salvo que sea necesario mantener esos datos, siquiera bloqueados, por así establecerlo una norma con rango legal o por así aconsejarlo un criterio organizativo para la mejor atención del servicio siempre que esa necesidad de conservación sea motivada y justificada.

Asimismo, habrá que tener en cuenta en este tipo de convocatorias la publicidad restringida de las mujeres beneficiarias, dado que una publicación en boletín oficial o en página web con carácter general vulneraría el principio de confidencialidad y vulneraría igualmente lo dispuesto en la LOPD y su Reglamento de desarrollo en cuanto a la seguridad de este tipo de datos personales.

Cualquier sistema de publicidad, aunque sea restringida, debe ser valorado de forma individualizada, analizando las posibilidades de acceso y, sobre todo, la imposibilidad de terceras personas de acceder a la información de una de las beneficiarias.

Para conseguir una actualización permanente de los datos personales en poder de las organizaciones, es aconsejable que éstas adopten un protocolo de revisión de estos datos, por ejemplo, mediante la puesta en contacto con la mujer víctima de violencia periódicamente para conocer su situación y si continúa requiriendo alguna atención del servicio. Estos procesos de actualización de datos pueden consistir en una puesta en contacto periódica con la mujer (semestral o anual) que permita confirmar su situación y su condición o no de ser susceptible de recibir cualquiera de los servicios ofertados por la administración competente. En esa puesta en contacto, sería conveniente que la mujer fuera informada de la posibilidad de proceder a la cancelación de sus datos personales.

Si la puesta en contacto no fuera posible, por ejemplo, porque no sigue empadronada en el municipio, no es válida su dirección, teléfono u otras formas de contacto, o ha resultado infructuoso el intento de contacto, o ha transcurrido un período de tiempo razonable sin tener otras noticias de ella, se puede proceder a la cancelación de oficio de los datos.

Es posible que un servicio administrativo ponga reparos a la cancelación ya que puede necesitar con posterioridad la información que obra en el fichero. En estos casos, y si la finalidad está justificada, es posible el mantenimiento de los datos, pero siempre debemos tener presente que no es posible guardar los datos simplemente por tenerlos, o "por si acaso".

La determinación temporal durante la cual los datos deben ser mantenidos requiere que sea fijada por el organismo, y finalizado este período, procederá la cancelación de los datos. Igualmente, hay que tener en cuenta que pueden existir requerimientos legales o contractuales o atender responsabilidades derivadas del propio tratamiento que obliguen al mantenimiento del fichero en un determinado alcance temporal, como por ejemplo, la legislación sanitaria que obliga a mantener las historias clínicas un período mínimo de cinco años.

En estos casos, los datos deben ser bloqueados hasta que transcurran esos plazos, siendo entonces cuando los datos quedarán definitivamente cancelados mediante destrucción física o técnicas de disociación que no permitan la identificación de la persona titular de esos datos, eliminando sus referencias identificativas.

6. GARANTÍA DE LOS DERECHOS ARCO

6. ¿CÓMO SE GARANTIZA EL EJERCICIO DE LOS DERECHOS ARCO?

Los denominados derechos ARCO son el conjunto de derechos - de acceso, de rectificación, de cancelación y de oposición- a través de los cuales la LOPD garantiza a las personas el poder de control sobre sus datos personales.

Se trata de derechos cuyo ejercicio es personalísimo, de modo tal que sólo pueden ser ejercitados por la persona titular de los datos, por su representante legal o por otra persona física que acredite ostentar su representación. Derechos de los que la persona ha de ser informada en el momento en que se recaban sus datos personales.

La dificultad en la adecuada atención de estos derechos no deriva del procedimiento en sí mismo por cuanto está tasado por la ley, sino de la atención correcta de ese procedimiento en tanto requiere una ocupación personalizada a cada solicitud, una comprobación puntual, una resolución en plazos breves, una respuesta certera y un empleo de tiempo y dedicación.

PRIMERA CUESTIÓN:

¿CUÁNDO DEBEMOS INFORMAR A LA MUJER QUE ENFRENTA VIOLENCIA DE SUS DERECHOS EN RELACIÓN CON EL TRATAMIENTO QUE SE HACE DE SUS DATOS PERSONALES?

Como acabamos de mencionar, la normativa de protección de datos reconoce un conjunto de derechos, los denominados derechos ARCO, a las personas físicas de quienes se recaban sus datos personales, por medio de los cuales pueden ejercer el control sobre sus datos.

Estos derechos ARCO deben ser comunicados en el momento en que se procede a la recogida de los datos personales por cualquiera de los medios a través de los que la organización o entidad recoja datos personales (atención telefónica, presencial, mail, web o una aplicación móvil), de modo tal que la persona sea informada previamente a la recogida de sus datos de la posibilidad de ejercitar sus derechos ARCO y el medio a través del cual ejercitarlo.

El ejercicio de estos derechos ARCO se debe llevar a cabo a través de medios sencillos y gratuitos puestos a disposición de las personas usuarias, estando sujeta a plazos determinados y breves su resolución. Por ello, es necesario establecer procedimientos para su regulación. Si la persona solicitante cree que sus derechos en esta materia no han sido atendidos en forma y plazo según la normativa vigente, o la respuesta es insatisfactoria, puede recabar la tutela de las autoridades de control que en el caso de las instituciones vascas es la Agencia Vasca de Protección de Datos (AVPD).

Para garantizar el ejercicio de dichos derechos los organismos y entidades de la administración deben facilitar a su personal los formularios para que estén a disposición de las personas usuarias, y una adecuada formación que permita trasladar a las personas asistidas la información necesaria. Además, el personal que desde los distintos servicios trabajan con datos personales de personas físicas deben saber que tienen que ofrecer esta información, que deben tener a disposición de las personas formularios de cada uno de esos derechos, bien en papel o bien en la aplicación informática que permita extraerlos, así como en todos aquellos medios a través de los cuales el servicio puede recabar datos personales como es el mail, la página web o una aplicación móvil en su caso.

SEGUNDA CUESTIÓN:

¿QUÉ PROCESO DEBEMOS SEGUIR ANTE EL EJERCICIO DE DERECHO PERSONAL ARCO?

Ante el ejercicio de un derecho ARCO por una mujer a la que hemos atendido, el organismo o servicio administrativo debe contar con un protocolo de actuación tasado que establezca todos los pasos a seguir desde la recogida de la solicitud a la notificación de la resolución.

El primer paso que ha de seguir el personal que reciba una solicitud de ejercicio de un derecho ARCO (derechos de acceso, rectificación, cancelación y oposición al tratamiento de los datos personales propios) es saber a qué organismo o a qué persona del servicio debemos remitir la solicitud. Dada la complejidad, el tiempo que requiere su análisis frente a la brevedad de los plazos de resolución (un mes para resolver el derecho de acceso y diez días los de rectificación, cancelación y oposición) las organizaciones suelen contar con un departamento de atención de derechos ARCO atendido por profesionales expertos. Cuando en el servicio de atención a derechos ARCO establecido se reciba una petición de acceso, se deberá poner sello o firma y fecha de recepción, para tener constancia del plazo para la contestación y remitirá la solicitud al personal competente para su tramitación y resolución que, recibida la solicitud, verificará si cumple con los requisitos mínimos:

1) Nombre y apellidos de la persona interesada.

2) Fotocopia de su D.N.I., pasaporte, N.I.E. o cualquier otra identificación que acredite suficientemente su identidad y, en su caso, de la persona que lo representa. Si la solicitud se realiza por medios telemáticos será válida la firma electrónica identificativa.

3) Dirección a efecto de notificaciones.

4) Fecha y firma de la solicitud.

5) Contenido de la solicitud.

En el caso de que la solicitud no reúna los requisitos especificados en el apartado anterior, el o la responsable del fichero deberá solicitar la subsanación de los mismos. El plazo para la subsanación del mismo será de 10 días.

Hay que insistir en que el ejercicio de estos derechos ARCO es personalísimo, por lo que sólo podrá solicitarlo la persona interesada, sin perjuicio de que pueda designar a una persona representante. Es por ello que el personal competente para la atención de estos derechos deberá observar esta circunstancia y denegar la solicitud en caso contrario.

El personal de atención de derechos ARCO verificará la identidad de la persona interesada y que efectivamente ésta figura en las bases de datos de la organización, y obtendrá la siguiente información del solicitante:

- Información de los datos (datos que se tienen registrados).
- Origen de los datos.
- Comunicaciones realizadas de los datos o que se prevén realizar de los mismos.

Una vez obtenida esta información, el personal de Atención de derechos ARCO enviará a la persona solicitante la información a través de correo certificado u otra forma de comunicación que permita dejar constancia de su recepción como el correo electrónico, siendo responsable de conservar la documentación que soporta el proceso.

7. RESUMEN

7. RESUMEN

— DE LA RECOGIDA DE INFORMACIÓN. En la recogida de la información de mujeres víctimas de violencia, hay que seguir de forma estricta las indicaciones sobre qué información hay que dar a estas mujeres.

— REQUISITO NECESARIO PARA LA RECOGIDA DE INFORMACIÓN. Es preciso antes de recoger la información, proceder a la declaración y constitución del fichero correspondiente donde se van a guardar esos datos.

— DEL CONSENTIMIENTO. El consentimiento será el mecanismo esencial previo a la recogida de información, y como recomendación general, debe ser recogido de forma expresa y por escrito, guardando dicho consentimiento a efectos de acreditarlo posteriormente.

— DEL TRATAMIENTO DE LOS DATOS. Debe ser respetuoso con el principio de calidad y de finalidad, no recogiendo más datos de los necesarios para la finalidad que se busca conseguir con dicho tratamiento.

— DE LA CESIÓN DE LOS DATOS. Sólo será posible en estos tres supuestos: 1) en caso de consentimiento de la persona titular de los datos personales 2) en caso de habilitación legal (una habilitación expresa en virtud de una norma con rango legal) o 3) porque se trate de comunicación de datos entre órganos con competencias iguales o sobre las mismas materias.

— DE LA CONSERVACIÓN DE LOS DATOS. Los datos deben ser guardados con la debida seguridad, que en el caso de las mujeres víctimas de violencia, debe ser la máxima prevista en la ley, es decir, las medidas de seguridad de nivel alto.

— DE LA CANCELACIÓN DE LOS DATOS. Los datos no pueden permanecer en poder de la organización más tiempo del estrictamente necesario para la finalidad que se buscaba originariamente, cancelando los mismos cuando dicha finalidad se cumpla.

— DEL EJERCICIO DE DERECHOS ARCO (ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN). El personal debe, por una parte, conocer el protocolo establecido por la organización para el ejercicio de estos derechos personales por las personas titulares de la información y, por otra, saber trasladar la información correspondiente a quienes la soliciten así como remitir las peticiones al órgano o servicio establecido para su resolución.

8. BIBLIOGRAFÍA Y DOCUMENTACIÓN

8. BIBLIOGRAFÍA Y DOCUMENTACIÓN

BIBLIOGRAFÍA

Agencia Española de Protección de Datos. Guía de Seguridad. 2014.

Agencia de Protección de Datos de la Comunidad de Madrid. Protección de Datos Personales para Administraciones Locales.

Agencia Vasca de Protección de Datos. Las Luces Funcionan… Cumpliendo con la Protección de Datos Personales, 2007.

Aparicio Salom, J. Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal. Aranzadi, 2009.

Cabrera Mercado, R. y Carazo Liébana, M. J. Análisis de la Legislación Autonómica sobre Violencia de Género. Ministerio de Igualdad, 2010.

Colin J. Bennett. En Defensa de la Privacidad.

Consejo General del Poder Judicial. La Importancia del Derecho a la Información de las Víctimas de Violencia de Género en la Ley Orgánica 1/2004 de 28 de diciembre de Medidas de Protección Integral contra la Violencia de Género.

Documentos de trabajo del Grupo del artículo 29 de la Directiva 95/46/CE.

El Derecho a la Protección de Datos Personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico. Revista de Derecho Comunitario Europeo.

Fernández Salmerón, M. Algunas Reflexiones acerca de la Protección de Datos en las Administraciones Públicas.

Goizueta Vertiz, J., González Murua, A. R y Pariente de Prada, I. El Espacio de Libertad, Seguridad y Justicia: Shengen y Protección de Datos. Euskal Herriko Unibertsitatea-Universidad del País Vasco, 2014.

Guía de los Derechos de las Mujeres Víctimas de la Violencia de Género. Ministerio de Sanidad, Servicios Sociales e Igualdad.

Guichot Reina, E. Publicidad y Privacidad de la Información Administrativa. Thomson-Civitas.

Guichot Reina, E. Acceso a la Información y Protección de Datos. Estado de la cuestión.

Guichot Reina, E. Datos Personales y Administración Pública. Thomson-Civitas.

Guichot Reina, E. La Comunicación de Datos Personales en Poder de la Administración. Aspectos Generales y Especialidades derivadas de la Comunicación por Vía Telemática.

Guichot Reina, E. La Potestad Sancionadora en Materia de Protección de Datos: Aproximación General.

Guichot Reina, E. La Potestad Sancionadora de la Agencia Española de Protección de Datos. Thomson-Aranzadi.

Lacaste, R., Sanmartín, E. y Velasco, J.. Auditoría de la Protección de Datos. Bosch.

Messia de la Cerda, J. A. La Cesión de Datos de Carácter Personal. Civitas.

Saiz Peña, C. A. Aproximación a los Aspectos de Protección de Datos, Riesgos Contractuales y Análisis de Riesgos de Seguridad de la Información.

Serrano Pérez, M. M. El Derecho Fundamental a la Protección de Datos, Derecho Español y Comparado. Thomsom-Civitas.

Troncoso Reigada, A. La Contribución de las Agencias Autonómicas al Derecho Fundamental a la Protección de Datos.

Troncoso Reigada, A. La Protección de Datos Personales: en Busca del Equilibrio. Tirant lo Blanc.

Valero Torrijos, J., Fernández Salmerón, M. y Parra Sáez, S. Crónica sobre la Protección de los Datos Personales en las Administraciones Públicas.

Villaverde Menéndez, I. Protección de Datos Personales, Derecho a Ser Informado y Autodeterminación Informativa del Individuo.

PROTOCOLOS Y GUÍAS DE ACTUACIÓN ANTE LA VIOLENCIA EN LA COMUNIDAD AUTÓNOMA DE EUSKADI

EUDEL. Guía de Pautas para la Adopción de Protocolos Locales y Medidas para la Mejora en la Atención a Mujeres Víctimas de Maltrato Doméstico y Agresiones Sexuales.

Abanto Zierbena. Protocolo Violencia de Género.

Balmaseda. Protocolo de Actuación para la Mejora en la Atención a Mujeres Víctimas de Violencia de Género.

Basauri. Protocolo Municipal de Coordinación Interinstitucional para la Atención a Mujeres que han sufrido Agresiones Sexuales y Malos Tratos en Basauri.

Bilbao. Protocolo Municipal de Coordinación para la Atención Integral en Situaciones de Violencia de Género entre las Áreas de Acción Social, Seguridad Ciudadana y Protección Civil y Mujer y Cooperación al Desarrollo.

Busturialdea-Gernika-Lumo. Acuerdo Comarcal de Actuación para la Mejora en la Atención a Mujeres Víctimas de Maltrato en el Ámbito Doméstico y de Violencia Sexual.

Donostia-San Sebastian. Protocolo Municipal de Intervención con Mujeres Víctimas de Violencia Machista.

Duranguesado (Abadiño, Berriz, Durango y Elorrio). Protocolo de Coordinación Interinstitucional del Duranguesado para la Mejora en la Atención a Mujeres Víctimas de Violencia Sexista.

Eibar. Protocolo Local de Actuación y Coordinación Interinstitucional para la Mejora en la Atención a Mujeres Víctimas de Maltrato en el Ámbito Doméstico y Violencia Sexual.

Elgoibar. Protocolo de Actuación Municipal y Coordinación interinstitucional para la Mejora de la Atención a las Mujeres Víctimas de Violencia de Género y Agresiones Sexuales.

Erandio. I Protocolo municipal de actuación y coordinación para casos de violencia de género y agresión sexual.

Ermua. Protocolo Local de Actuación y Coordinación Interinstitucional para la Mejora en la Atención a Mujeres Víctimas de Violencia de Género y Agresiones Sexuales.

Galdakao. Protocolo Local de Coordinación Interinstitucional en Casos de Violencia contra las Mujeres.

Hernani. Emakumeen Aurkako Indarkeriari Erantzuteko Udalerri-mailako Protokoloa.

Legazpi. Indarkeria Arreta Protokoloa.

Leioa. Protocolo de Coordinación en la Prevención y Atención de Victimas en Violencia de Género.

Muskiz. Protocolo Local de Actuación y Coordinación Interinstitucional para la Mejora en la Atención a Mujeres Víctimas de Violencia Sexista.

Ondarroa. Erakundeen Arteko Jarduerarako eta Koordinaziorako II Udal Protokoloa. Genero Indarkeriaren eta Sexu Erasoen Biktima diren Emakumeei Arreta Hobea Emateko.

Orozko. Protocolo Municipal de Atención Integral con las Mujeres que sufran Malos Tratos y Agresiones Sexuales.

Santurtzi. Protocolo de Actuación y Coordinación Interinstitucional para Mejora en la Atención a las Mujeres Víctimas de Violencia Género y Agresiones Sexuales.

Tolosa. Primer Protocolo Local de Actuación y Coordinación Interinstitucional para la Mejora en la Atención a Mujeres afectadas por Violencia de Género y Agresiones Sexuales.

Uribe Kosta. Protocolo de Coordinación en Materia de Violencia contra las Mujeres.

Urola Garaia (Ezkio-Itsaso, Legazpi, Urretxu eta Zumarraga). Erakundeen Arteko Koordinaziorako Urola Garaia Udal Elkartearen I Protokoloa Genero Indarkeriaren eta Sexu Erasoen Biktima diren Emakumeei Arreta Hobea Emateko.

Vitoria-Gasteiz. Protocolo Municipal de Intervención, Derivación y Seguimiento a Mujeres Víctimas de Violencia Doméstica y de Género.

RESOLUCIONES E INSTRUCCIONES DE LAS AUTORIDADES DE CONTROL, QUE FIJAN LA DOCTRINA EN MATERIA DE PROTECCIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PERSONAL, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) Y AGENCIA VASCA DE PROTECCIÓN DE DATOS (AVPD) Y DE LA RELATIVAS A:

INFORMES DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS:

Informe AEPD 453/2006, sobre cesión de datos de violencia de género a la autoridad judicial.

Informe 453/2006, sobre secreto de datos de las mujeres víctimas de violencia de género

Informe AEPD 183/2009, sobre restricción del acceso a datos personales por personal público a fin de evitar que pueda llegar a ser conocido por los agresores (Informe AEPD 183/2009),

Informe AEPD 320/2008, sobre medidas de seguridad en ficheros no automatizados

Informe AEPD 21/2009, sobre utilización de la misma clave de acceso al equipo informático.

Informe AEPD 183/2009, sobre medidas de seguridad en ficheros relativos a la violencia de género.

Informe AEPD 584/2009 sobre medidas de seguridad aplicable al nivel alto

INFORMES Y DICTÁMENES DE LA AGENCIA VASCA DE PROTECCIÓN DE DATOS:

Informe AVPD DE 20/1/2011, sobre legalidad de mecanismos de coordinación de la atención a las víctimas de violencia de género en Euskadi.

Informe AVPD de 27/10/11, sobre mecanismos y procedimientos de intervención y derivación para la atención a mujeres víctimas de maltrato (Dictamen 11-029).

Dictamen AVPD de 9/8/2010, sobre la consideración de mismas o idénticas competencias en materia de servicios sociales.

Dictamen AVPD de 14/2/12, sobre nivel de seguridad de ficheros de comunicación.

Dictamen AVPD de 16/7/12, sobre convenio de colaboración entre Ayuntamientos y Lanbide.

Dictamen AVPD de 26/7/12, sobre conocimiento de datos especialmente protegidos de integrantes de bolsas de trabajo.

Dictámenes AVPD de 5/9 y 20/11/12, sobre cesión de datos de salud.

Dictamen AVPD de 11/9/12, sobre acceso a datos personales en proceso selectivo.

Dictamen AVPD de 9/5/2013, sobre acceso a información de las Administraciones Públicas vía telefónica.

Dictamen AVPD de 23/7/13, sobre cesión de datos personales entre instituciones.

Dictamen de 26/8/13, sobre acceso a expediente administrativo.

Dictamen AVPD de 19/9/13, sobre tratamiento de datos personales de beneficiarios de justicia gratuita.

Dictamen AVPD de 26/11/13, sobre acceso a datos personales procedentes de archivos y registro.

Dictamen de 30/11/13, sobre suministro de datos para estadísticas.

Dictamen AVPD de 21/12/13, sobre tratamiento de datos personales en virtud de convenios de colaboración.

Dictamen AVPD de 30/12/13, sobre acceso a la historia clínica por centros sociosanitarios.

Dictamen AVPD de 24/2/14, sobre cesión de registro de entradas y salidas.

Manual de buenas prácticas de protección de datos de la AVPD: decálogo de obligaciones.

9. GLOSARIO DE TÉRMINOS

9. GLOSARIO DE TÉRMINOS

Autenticación: procedimiento de comprobación de la identidad de un usuario o usuaria.

Bloqueo: la identificación y reserva de datos de carácter personal con el fin de impedir su tratamiento excepto por parte de las Administraciones públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades.

Cesión de datos: toda revelación de datos realizada a persona distinta de la persona física titular de los datos personales.

Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a una tercera persona, física o jurídica, para el cumplimiento de fines directamente relacionados con las funciones legítimas de la persona cedente y de la cesionaria con el previo consentimiento de la persona titular de la información.

Consentimiento: manifestación de voluntad, libre, inequívoca, específica e informada, por la cual la persona consiente el tratamiento de sus datos personales.

Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Datos Personales: cualquier información concerniente a personas físicas identificadas o identificables.

Destinatario o cesionario de datos personales: persona física o jurídica, de naturaleza pública o privada, a la que se revelen los datos personales.

Encargada del tratamiento: persona física o jurídica, de naturaleza jurídica o privada, que trate datos personales por cuenta de la persona responsable del fichero.

Fichero: todo conjunto organizado y estructurado de datos personales, accesibles con arreglo a criterios determinados. El mero cúmulo de datos sin criterio alguno no podrá tener la consideración de fichero a los efectos de la Ley.

El Fichero es automatizado cuando los datos se encuentran almacenados en dispositivos informáticos (discos duros, ordenadores, DVD…) que requieren de herramientas capaces de descifrar la información que contienen para su tratamiento, se habla de ficheros automatizados.

El Fichero es manual (no automatizado) en el caso en que el conjunto de datos estén almacenados en soportes que no requieren de herramientas para su tratamiento, como el papel. Se habla de fichero no automatizado o manual siempre y cuando el fichero esté estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales. Se incluyen en esta definición archivos donde se recojan de forma estructurada documentos en papel del tipo, por ejemplo, currículum vitae de candidaturas.

El Fichero es mixto cuando la misma información se recoge en forma automatizada y también manual.

En este concepto de "información" se contienen datos numéricos, alfabéticos, gráficos, fotográficos y acústicos, concepto que junto con su referencia a personas físicas "identificadas o identificables" delimita el concepto de datos personales a aquella información que pueda vincularse a una persona física de forma que sirva para reconocerla, localizarla y, en definitiva, identificarla o hacerla identificable frente al resto de las personas. Por lo tanto, y como una primera aproximación a la cuestión, el elemento determinante para identificar si nos encontramos ante un dato de carácter personal es que la información, por sí misma o combinada, permita conocer datos de una persona concreta, bien por estar directamente identificada a través de algún dato, o bien porque pueda llegar a identificarse por otro medio.

Ficheros temporales: ficheros de trabajo creados por personas usuarias o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento de datos personales.

Fuentes accesibles al público: a los efectos de la LOPD se consideran 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. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.

Identificación: procedimiento de reconocimiento de la identidad de un usuario o usuaria.

Medidas de seguridad: son las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza

de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

Persona interesada o afectada: es la persona física titular de los datos que sean objeto de tratamiento.

Procedimiento de disociación: todo tratamiento de datos personales que permita la obtención de datos disociados.

Responsable del fichero: es la persona, física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Por lo que respecta a las obligaciones a que está sometida la persona responsable del fichero, ésta decide sobre la creación del fichero, la finalidad, contenido y uso de los datos almacenados en ese fichero, además debe dar respuesta a las personas físicas cuando ejerciten ante la persona responsable sus derecho ARCO y también deberá adoptar las medidas de seguridad del fichero ya sean de nivel básico, medio o alto.

Responsable de seguridad: persona o personas a las que la persona física o jurídica responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad. Su función es proteger y salvaguardar la información sensible dentro de la empresa.

Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

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.

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

Supresión: la eliminación física de los datos de carácter personal bloqueados una vez cumplido el plazo de prescripción de las posibles responsabilidades nacidas del tratamiento durante el cual se guardaron bloqueados.

Tratamiento de datos personales: operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Para considerar que estamos ante un tratamiento de datos personales sometido a la protección de la LOPD es preciso que las operaciones descritas se realicen de forma automatizada o, si se realizan manualmente, que los datos personales se almacenen en un fichero entendido como un conjunto ordenado de datos.

Son ejemplos de tratamiento:

- La recogida de impresos de solicitud de inscripción.
- La grabación en una aplicación informática (fichero) de la cita concertada por una persona usuaria para entrevistarse con una trabajadora social.
- La obtención de nuevos datos a partir de la información recabada (calificación en uno u otro recurso asistencial).
- La actualización de la información existente en un fichero a partir de los nuevos datos recabados.
- La eliminación de los datos existentes en un fichero.
- La mera consulta de datos de un fichero.
- Facilitar el acceso a los datos de una persona física por parte de una tercera persona física o jurídica, mediante cualquier tipo de comunicación, consulta, interconexión o trasferencia (envío a una empresa proveedora o colaboradora de un grupo de personas usuarias para la realización de una actividad).

Usuario o usuaria: persona o, en su caso, 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 o usuaria física.

ANEXOS

ANEXOS

ANEXO 1: CLÁUSULA DE CONSENTIMIENTO INFORMADO PARA LA RECOGIDA Y CESIÓN DE DATOS PERSONALES

(IDENTIFICACIÓN Y LOGO DEL SERVICIO)

Dña.....conDNI/Pasaporte/Permiso de residencia/ Otro documento de identificación....., por medio del presente documento dejo constancia expresa de haber sido informada de los siguientes contenidos por el personal del Departamento/Diputación Foral/Ayuntamiento/Mancomunidad de .....:

1. Que mis datos personales serán incorporados y tratados en un fichero denominado ..... titularidad del Departamento/Diputación Foral/Ayuntamiento/ Mancomunidad de ..... con domicilio en ....., cuya finalidad es gestionar los datos personales necesarios para prestarme una atención integral –para la atención de quienes enfrentamos la violencia contra las mujeres– a mí así como a las personas que de mí dependen.

2. Que tengo derecho a negarme a facilitar esta autorización habiéndoseme comunicado las consecuencias que esta negativa puede tener.

3. Que podré ejercer gratuitamente los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) ante el Departamento/Diputación Foral/Ayuntamiento/Mancomunidad de ....., enviando una comunicación a la dirección más arriba indicada con la referencia "protección de datos", o cumplimentando en el Departamento/Diputación Foral/Ayuntamiento/Mancomunidad los formularios dispuestos al efecto o por medio de correo electrónico .....

4. Que esta información ayudará en la elaboración de políticas públicas basadas en datos objetivos y podrá ser utilizada para finalidades estadísticas y de investigación.

5. Que mis datos serán tratados con la confidencialidad exigida en la normativa en materia de protección de datos y con las medidas de seguridad exigidas en la misma.

6. Que he sido debidamente informada de cuanto antecedentemente se expone.

Y para que conste y surta los efectos oportunos, firmo la presente a fecha de.....

Firma de la mujer.

Identidad y firma de la persona que le acompaña dejando constancia del motivo de su asistencia.

CONSENTIMIENTO INFORMADO PARA LA CESIÓN DE DATOS PERSONALES

Asimismo manifiesto haber sido informada de que mis datos personales podrán ser comunicados o cedidos a las entidades, públicas o privadas, que, relacionadas en el reverso de este documento (6) y que señalo expresamente, con la finalidad de prestarme una atención integral a mí así como a las personas que de mí dependen, y sin perjuicio de la cesión que corresponda efectuar conforme a lo ordenado por la ley.

Conforme a todo ello, otorgo libremente mi consentimiento para la cesión de los datos personales necesarios a tales fines a favor de las entidades mencionadas en el reverso del presente documento, conforme a lo dispuesto en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

Y para que conste y surta los efectos oportunos, firmo la presente (7).

Fecha y firma de la mujer.

Identidad y firma de la persona que le acompaña dejando constancia del motivo de su asistencia.

CONSENTIMIENTO INFORMADO EN CASO DE PRESENCIA DE MENORES

Siendo mi hija/hijo menor de 14 años, doy mi consentimiento como madre/tutora para la recogida de sus datos personales y su cesión a las entidades mencionadas, autorizando el tratamiento de los mismos a efectos y finalidad señalada.

Y para que conste y surta los efectos oportunos, firmo la presente.

Fecha y firma de la mujer.

Identidad y firma de la persona que le acompaña dejando constancia del motivo de su asistencia.

---

(6) Muy importante: en este punto hay que indicar la relación de entidades a las que para la finalidad asistencial serán o podrán ser cedidos. La mención a cada una de esas entidades deberá ir precedida de una casilla que permita marcar a qué administraciones o servicios consiente la interesada dar la información (ver página 92). Esta casilla será marcada por el personal competente en previsión de las necesidades de atención de la mujer. Se trata de que de forma mecánica la técnica o técnico marquen las casillas a las que su conocimiento y experiencia indiquen que van a ser servicios que la atención a cada mujer requiera y que van a necesitar una cesión de datos entre distintos organismos, personas o entidades, actuación que se integra de forma ágil y dinámica en la actuación de atención y asesoramiento y que garantiza el absoluto respeto a los derechos personales de las mujeres atendidas en el servicio. En el caso de que no se haya contemplado alguna cesión que devenga necesaria con posterioridad, habrá de emitirse nuevamente el documento completándolo con este nuevo consentimiento, para su firma, entrega y almacenamiento de la copia firmada.

(7) Deberá emitirse una copia del documento una vez firmado incluyendo el reverso en que figure las opciones marcadas para la cesión de datos personales.

CONSENTIMIENTO INFORMADO EN CASO DE GRABACIÓN (8)

He sido informada de que la recogida de información ha quedado registrada en soporte de audio/video/audio-video)para documentar la recogida de información.

Y para que conste y surta los efectos oportunos, firmo la presente.

Fecha y firma de la mujer.

Identidad y firma de la persona que le acompaña dejando constancia del motivo de su asistencia.

(8) Se trata ésta de una cláusula opcional para el caso en que se recoja información en soportes de grabación de audio y/o video. En este caso deberá incluirse una mención específica para el consentimiento de esa grabación con el contenido que se indica.

REVERSO

Marco las entidades a las que permito se cedan mis datos personales para una intervención integral y coordinada.

☐ Gobierno Vasco

- ☐ Seguridad (Ertzaintza)
- ☐ Políticas Sociales
- ☐ Vivienda
- ☐ Justicia
- ☐ Salud (Osakidetza)
- ☐ Educación
- ☐ Empleo (Lanbide)
- ☐ Igualdad (Emakunde)
- ☐ Ararteko

☐ Diputación Foral de_____

- ☐ Asuntos Sociales
- ☐ Casa de acogida de_____
- ☐ Servicio jurídico
- ☐ Servicio psicológico
- ☐ Servicio de infancia
- ☐ Servicio de Igualdad

☐ Servicios municipales del Ayuntamiento de _____

- ☐ Asuntos Sociales
- ☐ Casa de acogida de_____
- ☐ Servicio jurídico
- ☐ Servicio psicológico
- ☐ Servicio de igualdad

☐ SEPE Servicio Público de Empleo

☐ Otros servicios

- ☐ Asociación_____
- ☐ Escuela/colegio/Universidad _____
- ☐ Abogada o abogado_____

☐ Otros servicios (identificar expresamente)_____

ANEXO 2: FAQ-PREGUNTAS FRECUENTES PLANTEADAS POR EL PERSONAL TÉCNICO EN EL PROCESO DE EJECUCIÓN DE LA GUÍA

Las cuestiones que se contienen en el presente apartado han sido planteadas por trabajadoras y trabajadores que atienden a mujeres que enfrentan violencia. Han sido ordenadas conforme a la identificación de los distintos escenarios analizados en la presente guía en sus epígrafes I a VI.

1. INFORMACIÓN Y RECOGIDA DE DATOS PERSONALES

FAQ 1

CUESTIÓN PLANTEADA: **De acuerdo a la LOPD, ¿puede una entidad que se dedica a la atención psicológica recoger datos de alta sensibilidad como la discapacidad, el VIH o si esa mujer ejerce o no la prostitución?**

SÍ. Es una circunstancia natural que la atención psicológica requiera conocer datos como los indicados, algunos de los cuales son del más alto grado de sensibilidad. Son datos de alta sensibilidad (entre otros) los de salud física, como es el conocimiento del VIH, o los de salud psíquica.

Por lo que respecta a la diversidad funcional, el dato en sí de la discapacidad es un supuesto que la norma expresamente excepciona del nivel alto de protección y lo considera de nivel básico. Superado lo anterior, esto es, el porcentaje del grado de discapacidad o el diagnóstico determinante de la misma, sí son datos de nivel alto.

La diferencia entre un dato de nivel básico y un dato de nivel alto no afecta a su recogida, como se ha indicado antes. Naturalmente podrán recabarse siempre que sea necesario, en este caso, para prestar una adecuada asistencia psicológica. Y hay que tener en cuenta la finalidad para la que se recoge el dato; en el caso de la atención psicológica, si tiene una finalidad asistencial, curativa, etc.

La distinción afecta a las medidas de seguridad con que habrán de conservarse, almacenarse, manejarse, comunicarse los datos. Los datos personales de nivel alto deberán manejarse bajo medidas de seguridad de nivel alto. Ello significa que en su tratamiento y manejo se adoptarán medidas de nivel básico, medio y alto, por ser de carácter acumulativo.

Entre las medidas de nivel alto se encuentra el cifrado de los soportes y documentos de forma que dificulten la identificación de su contenido para el resto de personas ajenas a las

autorizadas para su manejo, y seguir ese criterio durante el transporte de los soportes que contengan esa información. Además, se deberá conservar una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan o utilizar elementos que garanticen la integridad y recuperación de la información. Asimismo, se registrará la información relativa a cada intento de acceso, entre otras cosas si ha sido autorizado o denegado. Se encriptará, además, las comunicaciones que transmitan este tipo de datos personales del más alto nivel, entre otras de las obligatorias medidas de seguridad de nivel alto que ordena la Ley.

2. TRATAMIENTO DE DATOS PERSONALES

FAQ 2

CUESTIÓN PLANTEADA: **De acuerdo a la LOPD, ¿puede una entidad que se dedica a un área de trabajo (por ejemplo la protección) recoger datos sobre campos que no son de su competencia (por ejemplo si trabaja o no) con el objetivo de unificar los datos y elaborar estadísticas comparables con las demás entidades?**

La cuestión aborda dos escenarios:

¿Puede una entidad en un área de trabajo determinada recoger datos ajenos a su competencia?

Sin embargo, la cuestión expuesta es en sí dudosa por cuanto si el área de trabajo es la protección puede que el dato personal sea necesario. Por lo tanto, la respuesta abordará ambos aspectos.

La utilización de los datos personales viene vinculada a la finalidad para la cual el servicio necesite recabar datos personales. Esto es, si el área de trabajo (en el ejemplo, la protección) requiere conocer el dato de si la víctima trabaja o no, será un dato necesario para la prestación de ese servicio.

Si el área de actividad no requiere conocer ese dato personal, se conculcará el principio de finalidad que exige el tratamiento de datos personales, que hace que no pueda recabarse ese dato. De ese modo, y en el ejemplo planteado no podrían recogerse datos con efectos estadísticos por cuanto no es ésa la función o finalidad del servicio ofrecido por la entidad. Por lo tanto, el elemento esencial para hacer esta valoración es la finalidad, y no el hecho de la competencia del órgano administrativo en cuestión.

¿Podríamos utilizarlos para finalidades estadísticas?

SI. Podrán ser usados para fines históricos, estadísticos o científicos, aunque no se recogiesen inicialmente con esta intención, si bien es necesario para este propósito que se anonimicen los datos personales. Además habrá que tener en cuenta la legislación vigente en materia estadística que determinará qué utilización puede darse de los datos personales y qué finalidad preside el propósito estadístico.

FAQ 3

CUESTIÓN PLANTEADA: **Un Ayuntamiento, en el marco del protocolo de atención a mujeres víctimas de violencia sexista, ha creado un sistema que mediante un logaritmo del DNI codifica la identidad de las mujeres atendidas (todas las entidades que participan en el protocolo realizan esta codificación). Así, las entidades (por ejemplo Lanbide) participantes informan a la coordinadora del protocolo que la mujer Xf3gd759 ha sido atendida. Este código no puede ser descodificado.**

Entonces dos cuestiones: 1) ¿incumpliría si la coordinadora ha tenido contacto previo con esa mujer y le figura el mismo código Xf3gd759 en un listado de su entidad? 2) ¿incumple esto la LOPD si la coordinadora no puede conocer de qué mujer se trata?

En el concepto de "dato personal" no existe una lista cerrada sino que lo integra todo dato, cualquiera que sea su naturaleza, que identifica o permite la identificación de una persona, quedando excluidos los datos disociados que son aquellos que no permiten la identificación de su titular.

Es proceso de disociación todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

Por lo tanto, el sistema diseñado por la coordinadora pretende ser un proceso de disociación. Así, efectuada esa disociación de datos personales mediante la asignación a una mujer de un código alfanumérico, la información podrá ser consultada por las personas interventoras en su asistencia sin poder identificar a la mujer.

De ese modo, la base de datos que recogiera esta información estaría totalmente anonimizada y, por tanto, quedaría excluida del ámbito de aplicación de la LOPD y su Reglamento que lo desarrolla al no constituir ya, en virtud de ese proceso, un dato personal. Ello exigiría una valoración específica del procedimiento de disociación y la irreversibilidad de la misma.

Si la labor que efectúa la coordinadora es la de organización y armonización de la asistencia que se le propone o que ha recibido una mujer no será necesario conocer su identidad en

los términos precedentemente indicados. De ese modo, la coordinadora podrá realizar su tarea organizativa sin tener por qué conocer de qué mujer se trata. La cuestión relevante es si de alguna forma es posible que esa persona pueda acceder a establecer una relación entre el código y el número de referencia.

Si la coordinación va más allá y requiere un análisis de la intervención y de su resultado hasta el punto de que la coordinadora ha podido tener trato con la mujer, ha anotado sus datos personales, y puede identificarla asociando el código con la persona, el proceso de disociación pierde su virtualidad.

Esto es, si la coordinadora necesita saber cuál es la identidad de la mujer y decodifica el número, el proceso de disociación queda revertido.

La Agencia Española de Protección de Datos señala que será suficiente en orden a la protección de los datos personales la posibilidad incluso remota de que, la información pueda revelar la identidad de las personas afectadas por los tratamientos de datos. Esto es, para la consideración como dato disociado, será necesario que de la aplicación de dicho procedimiento resulte imposible asociar un determinado dato con una persona determinada.

En consecuencia, si el sistema diseñado permite identificar a la mujer sin esfuerzos desproporcionados, el resultado que arroja no puede considerarse dato disociado -anónimo- sino dato personal o identificativo a todos los efectos.

FAQ 4

CUESTIÓN PLANTEADA: **Recientemente se ha atendido a una mujer víctima de una agresión sexual perpetrada por su ex pareja y, además, víctima de una agresión por parte de otra mujer; en la orden de protección, aparecen los nombres de las dos personas. La mujer presunta agresora, es también usuaria de servicios sociales y tiene un menor a cargo, cuya situación es de riesgo y desde el servicio de infancia se está haciendo una valoración del caso. La víctima contó (y denunció) que la agresora es consumidora habitual de drogas y estaba bajo los efectos de éstas en el momento en que se produjo la agresión.**

La duda que se plantea es si los datos de las presuntas personas agresoras se pueden utilizar, teniendo en cuenta el interés del menor, o si de acuerdo a la LOPD esta información no se puede utilizar. Se plantea la duda de si se debe informar al servicio de infancia de que la madre del menor, ha sido denunciada por agresión y que estaba bajo los efectos de las drogas.

A la complejidad del ámbito de la violencia, se suma el específico de la protección de datos que requiere de un especial cuidado y diligencia. Además, hay que tener en cuenta la rele-

vancia del conocimiento de datos judiciales que revelan o pudieran revelar aspectos delictivos.

Antes de responder a la cuestión, pongámonos en situación.

Los **hechos principales** que plantea la cuestión son los siguientes:

— Acude una mujer víctima de una agresión a ser atendida a los servicios sociales del ayuntamiento.

— Las personas agresoras son dos: un varón que es su ex pareja y una mujer.

— Por lo que respecta a la mujer víctima ya tiene iniciado un procedimiento penal por estos hechos, ya que tiene una orden de protección contra las personas autoras de la agresión.

— os servicios sociales disponen de una copia de esa orden de protección (probablemente se la ha facilitado la mujer víctima).

— El hombre habría agredido a su expareja (es un caso de violencia de género la agresión de otra mujer a la mujer víctima no es un supuesto de violencia de género).

— Los datos de la agresora (que incluirán el hecho de que tiene un menor a cargo, y todos los datos relacionados con la intervención de los servicios sociales) ya están en poder del servicio municipal, ya que es usuaria de los mismos.

— Durante la asistencia a la víctima, ésta les refiere datos personales de la agresora. Estos datos no tienen relación directa con la agresión o sus circunstancias sino con la situación social de la agresora y de su hijo. También les refiere datos de terceros que sí tienen relación con los hechos, como el que estuviera bajo los efectos de las drogas en el momento de la agresión (hecho que debe referirse a la policía, para incluirlo en el atestado).

Sentadas estas bases,

Primero:

La información que puede recoger el Servicio de Atención Social en relación con la agresión se debe limitar al hecho que motiva la asistencia, que es la agresión sexual. En este contexto, es donde la víctima refiere los datos de terceros que pasan a formar parte del expediente administrativo asistencial que se tramita a continuación.

Por lo tanto, no teniendo relación directa con el hecho que motiva la atención, la situación de la agresora queda fuera de la atención.

Hay que entender que una atención social debe centrarse en las circunstancias que la motivan. De ese modo, la recogida de información personal debe limitarse a dicha finalidad, que es la que preside toda la intervención.

Podemos entender que haya que valorar las circunstancias sociales de la víctima, para poder ampliar o mejorar la atención, pero no es de recibo que esto conlleve la recogida de información de terceros, como es el hijo menor de la agresora.

Segundo:

La entrevista y recogida de información no puede extenderse más allá de estas circunstancias. Tampoco se podrán recoger estos datos por escrito u otros medios, ni incorporarlos al fichero de datos de víctimas de violencia de género, por no estar directamente relacionados con aquellas circunstancias necesarias para valorar la agresión y asistir a la víctima.

Tercero:

En cuanto, y con carácter general, a si los datos que nos da la víctima pueden utilizarse para finalidades distintas, la respuesta debe ser también negativa.

La LOPD es estricta en cuanto a que los datos personales sólo pueden utilizarse para finalidades concretas y conocidas por la persona que da sus datos. En este caso, la opción para utilizar los datos personales recogidos en el expediente para otras finalidades, será la petición del consentimiento informado, sin el cual no se pueden utilizar dichos datos para finalidades distintas.

En casos concretos, se prevé que la cesión de estos datos a otros servicios o a otras administraciones puede hacerse sin ese consentimiento, y para eso debe haber una norma de rango legal (no es suficiente un protocolo, un reglamento o un Decreto de Alcaldía, por ejemplo) que lo habilite.

A modo de ejemplo, se autoriza la cesión de datos a policías, fiscalía o juzgados siempre que sea con la finalidad de perseguir el delito.

Si las circunstancias de la agresora y el menor pudieran conllevar la existencia de un delito o falta, las personas que conocieran de ese hecho pueden comunicar los datos expuestos a la policía. En cualquier caso, habría que analizar si la normativa relacionada con la problemática de los menores, asistencia a los mismos, etc., permite dicha cesión de datos.

FAQ 5

CUESTIÓN PLANTEADA: **¿Quién puede tener acceso a la información sobre los casos de mujeres víctimas de violencia de género? ¿Todas las personas que se encuentran dentro del protocolo o puede tener acceso alguien más?**

En primer lugar, cuando se recogen datos de una víctima, esta recogida se hace con una finalidad determinada y única.

Esa recogida de información se debe hacer informando a la víctima adecuadamente, porque ésta debe saber qué uso se va a dar a la información que presta a la administración.

No es posible, sin su conocimiento y su consentimiento, que esa información se utilice para otros usos. La única posibilidad de cambiar la finalidad inicial sería la denuncia, si los hechos constituyen un delito. Para ello no es necesario el consentimiento.

Sin consentimiento, la otra posibilidad que se abre para que los datos que la víctima ha prestado a la administración sean cedidos es que haya una norma de rango legal que prevea dicha cesión. Por ejemplo, un artículo en una ley que establezca que los datos que recojan los servicios sociales, serán puestos en conocimiento de (…). Si eso no existe, no es posible la cesión.

Una tercera posibilidad de cesión se permitiría entre servicios sociales pertenecientes a distintas instituciones o entre estos y el servicio de igualdad siempre que las competencias obedecieran a una misma finalidad de atención a la persona; en este caso, mujer víctima de violencia de género.

Los protocolos en el ámbito municipal no habilitan la cesión de datos entre los participantes en el mismo. Es decir, no es suficiente con que haya un protocolo como amparo legal para la cesión. En todo caso, sin consentimiento o amparo en una norma de rango legal no se pueden ceder los datos.

La utilidad de los protocolos reside en la definición de mecanismos de colaboración y ayuda, pero debe ser la propia mujer víctima de violencia quien defina y autorice a quién se van a ceder dichos datos.

Así pues, deberíamos recoger previamente su consentimiento para la cesión, y además el consentimiento para cesiones concretas y no genéricas, definiendo con claridad a quién se va a ceder dichos datos para que la víctima lo conozca sin ninguna duda.

FAQ 6

CUESTIÓN PLANTEADA: **Dentro de un ayuntamiento y más concretamente dentro de un departamento de servicios sociales compuesto por una persona responsable del departamento, una responsable de negociado de servicios sociales y el personal técnico y administrativos, cuando llega un caso de violencia contra las mujeres ¿qué personas deben conocer los datos identificativos y la intervención que se está realizando con la misma?**

¿Es necesario que lo conozca la persona responsable del departamento? y ¿que su expediente pueda pasar de mesa en mesa por el personal administrativo?

¿Se debe dar información a la persona responsable del departamento, concejalías o al alcalde o alcaldesa?

La respuesta viene dada no por una disposición legal directa, sino por la aplicación de un principio esencial de la normativa sobre protección de datos, que es el principio de calidad, vinculado a la finalidad.

Inicialmente, la recogida de datos viene amparada por el consentimiento de la mujer que nos ha dado sus datos y la información sobre su situación, con una finalidad, que es la de atenderla, asesorarla y ayudarla.

Dentro de esa finalidad, en el servicio hay una serie de mecanismos de funcionamiento que pueden exigir la revisión de la información o de las resoluciones por la persona responsable del servicio, o pueden exigir, por el reparto de tareas, la intervención de varias personas.

Mientras se mantenga la finalidad en el tratamiento, esto no plantea problemas. Estos surgen cuando se cambia la finalidad, y se ceden los datos a otro servicio municipal que tiene otra finalidad distinta, por ejemplo, se ceden al servicio del padrón para verificar el domicilio y los convivientes, o a recaudación para otras verificaciones, o se ceden al concejal o concejala o al alcalde o alcaldesa. Esta cesión, no sería correcta.

FAQ 7

CUESTIÓN PLANTEADA: **Una asociación participa en una convocatoria de ayudas económicas. ¿Los datos de esa asociación pueden ser transferidos a otra organización para otros objetivos (por ejemplo para derivar a la misma a mujeres víctimas de violencia etc.)? ¿Son estos datos personales?**

En relación a esta consulta, hay que diferenciar los datos de la asociación (persona jurídica), y por lo tanto que no tiene protección de datos personales, de los datos de la Dirección, Junta, u otros cargos de la asociación, que sí la tienen.

En el caso de estos últimos, hay que ver de dónde se obtienen los datos, porque hay registros públicos a travçes de los que se puede acceder a ciertos datos.

La asociación, como persona jurídica, tiene que guardar y custodiar los datos de las personas socias y directivas con la misma confidencialidad y cautela que cualquier otra empresa u organización.

Y por último, los datos de domicilio, teléfono, etc. de la asociación, no están sometidos a la ley de protección de datos.

FAQ 8

CUESTIÓN PLANTEADA: **Existe un protocolo de actividad en una mancomunidad desde 2012. También está en marcha la Mesa Interinstitucional y nos coordinamos con la Ertzaintza y Osakidetza.**

Este año 2014, estamos elaborando el plan integral frente a la violencia de género y dentro de ello, también nos hemos coordinado con los alguaciles de los pueblos y hemos sabido que ellos también reciben las órdenes de protección, que les envían desde el juzgado, para hacer su seguimiento.

El problema es el tratamiento que les dan a las órdenes de protección en los municipios pequeños, o mejor dicho, la falta de tratamiento, es decir, en la mayor parte de los municipios una factura y una orden de alejamiento tienen el mismo procedimiento, sin confidencialidad alguna.

Cualquier organización, sea pública o privada, debe cumplir con la ley de protección de datos, que tiene unas exigencias importantes en relación con las víctimas de violencia de género, exigencias que son mucho más elevadas que en el caso de los datos "normales".

En el caso de la violencia de género la Ley exige por ejemplo, un nivel de protección de los datos con seguridad alta, que es realmente una seguridad muy difícil de cumplir.

Si estamos hablando de que en un ayuntamiento puede recibirse una orden de protección que va a ser tratada sin ninguna confidencialidad, el problema que se plantea es enorme, y puede conllevar responsabilidades importantes.

El tratamiento de los datos de víctimas de violencia en todas sus manifestaciones debe ser especialmente cuidadoso, precisamente para evitar perjuicios a las mismas.

Hay que implantar en los ayuntamientos una cultura de respeto de la protección de datos aunque sea mínima, que asegure que los datos de las víctimas se reciben y se tratan con respeto a unas mínimas medidas de seguridad.

FAQ 9

CUESTIÓN PLANTEADA: **Se amplía la anterior cuestión, interesando concretar un poco más el procedimiento a seguir, aunque sea como propuesta, o informar acerca de los artículos de la LOPD que se refieren a este tipo de datos.**

Vamos a intentar exponer ese escenario de una forma sintetizada que permita valorar la complejidad de este particular ámbito. Al final incluimos un decálogo de observaciones básicas que hay que tener en cuenta en el tratamiento de datos personales.

Entrando en el apartado de medidas de seguridad, el art. 81.3 del Reglamento de desarrollo de la LOPD señala que además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán, entre otros, a los ficheros o tratamientos de datos de carácter personal que contengan datos derivados de actos de violencia de género.

Así, del examen de las diferentes medidas de seguridad aplicables cabe destacar, en primer lugar, que el artículo 91 del Reglamento impone ya en los ficheros de nivel básico como una de las medidas de seguridad la del control de acceso, disponiendo en su número primero que "Los usuarios o usuarias tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones"; para ello exige en su número tercero que "El o la responsable del fichero establecerá mecanismos para evitar que un usuario o usuaria pueda acceder a recursos con derechos distintos de los autorizados."

Además, el número 2 especifica que "El o la responsable del fichero se encargará de que exista una relación actualizada de usuarios o usuarias y perfiles de usuarios o usuarias, y los accesos autorizados para cada uno de ellos o ellas. "

Asimismo, se establece una obligación de identificación y autenticación de los usuarios y usuarias, exigiéndose ya desde el nivel básico una identificación personalizada de estos. Dispone el artículo 93.1, a estos efectos, que "El o la responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de las o los usuarios." Por su parte, el número 2 del mismo artículo prevé que "El o la responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario o usuaria que intente acceder al sistema de información y la verificación de que está autorizado." Esta contraseña sólo debe ser conocida por la usuaria o usuario autorizado,

Además, el artículo 93.3 del Reglamento de desarrollo LOPD indica que "Cuando el mecanismo de autenticación se base en la existencia de contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad."

En el nivel medio, esta medida de identificación y autenticación se vuelve más rigurosa ya que, a las medidas anteriores previstas para el nivel básico, se añade la contenida en el artículo 98 según el cual habrá de contarse con "un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información."

Por último, en el nivel alto, se requiere ya un registro de cada intento de acceso que se produzca, y así establece el artículo 103.1 del Reglamento de desarrollo LOPD que "De cada intento de acceso se guardarán, como mínimo, la identificación del usuario o usuaria, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado." Mientras que el número segundo del mismo artículo dispone "En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido."

De ello se deriva que no todas las personas que respondan al perfil señalado en el artículo anteriormente transcrito tendrán acceso al fichero a que se viene haciendo referencia, sino solamente aquellas a quien se califique como usuarios o usuarias en un documento denominado Documento de Seguridad que es el manual donde, entre numerosos aspectos, se definen las funciones y obligaciones de cada uno de los usuarios y usuarios o perfiles de acceso a los datos de carácter personal y a los sistemas de información.

Estas personas deberán acceder con su contraseña, que como ya se ha señalado, debe ser personal y secreta sin que sean admisibles las contraseñas genéricas. Por último, para que pueda conocerse si alguien ha accedido a dicho fichero, y en su caso, quién, en qué momento y a qué información, deberá constar, en lo que el Reglamento de desarrollo de la LOPD denomina registro de accesos, cada uno de aquéllos que se haya producido.

La exquisita y detallada regulación de las actuaciones de todas aquellas personas que intervengan en la gestión de datos personales de una mujer que enfrenta un acto de violencia, hace que deban respetarse una serie de parámetros legalmente establecidos y que constitu-

yen un grado de mínimos. A los efectos de sintetizarlos se indica una relación concreta de esos parámetros:

1) Los datos personales pertenecen a las personas titulares de los mismos y sólo ellas pueden decidir sobre estos. Ni las trabajadoras o trabajadores del servicio, ni el servicio, ni el departamento al que pertenezca son dueños de esos datos.

2) Hay que informar y pedir el consentimiento, para lo cual hay que disponer de un formulario adecuado.

3) Hay que solicitar únicamente los datos adecuados, pertinentes y no excesivos a la finalidad para la que se recogen que ha de ser determinada y legítima, y no pueden usarse para finalidades distintas.

4) El deber de secreto y confidencialidad de los datos personales que se conocen con motivo del trabajo que se desarrolla es esencial. A ello obliga la normativa de protección de datos, el estatuto del funcionario público y una ética de conducta básica. En ocasiones, el incumplimiento, puede ser perseguido penalmente.

5) Hay que cumplir con las medidas de seguridad a que antes nos hemos referido. Esas medidas de seguridad deben estar indicadas en el Documento de Seguridad, que, por tanto, ha de ser de conocimiento del personal. A este respecto, hay que utilizar las contraseñas y no compartirlas; hay que guardar los expedientes o listados con datos personales en armarios, que deberán cerrarse cuando no se esté; hay que mantener los datos personales fuera de la vista de personas no autorizadas (particularmente hay que prestar atención a los documentos que se dejan en fotocopiadoras, impresoras, faxes o, incluso, encima de la mesa); hay que cumplir las medidas de seguridad que se hayan establecido en caso de extracción de soportes (nos llevamos trabajo a casa en memorias USB o en papel).

6) Hay que facilitar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) a las personas titulares de los datos personales.

7) Hay que prestar atención a la cesión de datos, hay que saber que sólo procede si contamos con consentimiento de la persona titular de los datos o si existe una norma con rango legal que lo permite. En el ámbito que analizamos no existe una previsión legal específica a este respecto.

8) Antes de facilitar datos personales a empresas o entidades que, en virtud de contratos, realizan trabajos para la organización (desarrollos informáticos, seguridad, limpieza, distribución de correspondencia, destrucción de documentos…) debemos asegurarnos que existe un contrato firmado donde se les imponen obligaciones de confidencialidad y de seguridad de la información respecto a los datos de carácter personal, por cuanto si no se-

remos responsables de la pérdida, fuga, desaparición, destrucción o sustracción de la información.

9) Cancelar los datos cuando dejen de ser necesarios o pertinentes para la finalidad para la cual fueron recogidos. Algunas veces, antes de destruirlos habrá que bloquearlos, esto es, imposibilitar el tratamiento y permitir el acceso sólo cuando se den algunas situaciones concretas. Para destruir ficheros con datos personales en soporte papel hay que utilizar las destructoras de papel o el sistema seguro que haya establecido la organización.

10) Hay que prestar atención al envío de datos personales a través del correo electrónico. Hay que señalar que los datos de violencia de género u otros especialmente protegidos como los datos de salud deben ser encriptados antes de remitirlos por este medio.

La complejidad de estas actuaciones hace imprescindible que las organizaciones contemplen la formación de su personal en seguridad de la información y protección de datos personales. Organizar actividades formativas que permitan al personal obtener conocimientos en esta materia, con análisis de escenarios prácticos de aplicación e incluso sesiones formativas específicas sobre temas de interés, favorecerá la concienciación de un adecuado tratamiento de la información personal.

FAQ 10

CUESTIÓN PLANTEADA: **Una entidad (A) cede unos datos personales a otra entidad (B) con el consentimiento de la mujer, etc. ¿Esta segunda entidad (B) puede ceder a su vez los datos a otra entidad (C) porque vea que puede ser de interés que esta última entidad (C) conozca la situación de la mujer?**

El interés debe interpretarse necesariamente como finalidad en la atención que requiere la mujer. Una vez definida la situación en estos términos, la entidad B ha de comprobar que cuenta con los requisitos de consentimiento de la mujer para, a su vez, ceder esos datos a la entidad C, o en su caso, analizar si existe una norma legal habilitante para la cesión o si se trata de competencias idénticas en atención a la finalidad de atención que requiere la mujer.

FAQ 11

CUESTIÓN PLANTEADA: **Una mujer es atendida por la policía de un municipio y una vez recogida la denuncia y, para que sea orientada/atendida, le dice que se dirija a Emakunde. Sin embargo, Emakunde no tiene estas competencias. La técnica de Emakunde le escribe un e-mail a la persona que coordina el protocolo de violencia en ese ayuntamiento y le informa de lo sucedido para que, si lo ven necesario, tomen las medidas oportunas. La persona responsable del protocolo de ese ayuntamiento llama a Emakunde y le solicita que le diga el nombre de la mujer que ha sido erróneamente derivada a fin de detectar qué profesional atendió a la mujer en la policía e informarle así al profesional para que en el futuro derive correctamente, ¿debe decirle el nombre de la mujer atendida?**

Rotundamente no.

El conocer el dato de la mujer que ha sido atendida para derivar responsabilidades o corregir una información incorrecta claramente excede el principio de proporcionalidad en el tratamiento de la información personal. Estaríamos ante una cesión para la cual no existe ninguna autorización ni legal, ni habilitante por competencias idénticas ni por supuesto consentida por la mujer.

La situación se resuelve de forma tan sencilla como tomar nota de la comunicación remitida por la técnica municipal y remitir desde Emakunde una circular a la policía poniendo en conocimiento de cuál es el proceso correcto y advirtiendo de que se han participado situaciones similares en las que se ha derivado incorrectamente a las mujeres atendidas.

FAQ 12

CUESTIÓN PLANTEADA: **Una mujer y una hija menor de edad son acogidas en un recurso residencial de la Diputación Foral porque en este momento no tienen dónde acudir. Las profesionales de ese recurso, al ser la hija menor de edad, llaman al padre de la criatura (que es quien está violentando a la madre y por extensión a la hija) para informarle de que su hija está acogida en el recurso y pedirle permiso para que esta niña reciba apoyo psicológico. ¿Deben en este contexto las profesionales del recurso informar al padre y solicitarle el permiso para la atención psicológica?**

La situación no puede ser distinta ni especialmente protegida porque se trate de una situación de violencia. Por lo tanto, se trata de simplificar la situación y actuar conforme se actuaría en una situación ordinaria; esto es, se podrá prestar la atención médica con el consentimiento de una de las personas progenitoras como en cualquier caso ordinario de atención médica a un o una menor fuera de una situación de violencia contra las mujeres. A mayor

abundamiento, la prestación de asistencia psicológica puede no obedecer a parámetros médicos; esto es, puede no ser entendida como una atención sanitaria en parámetros médicos.

En cualquier caso, si las agresiones se estuvieran produciendo directamente sobre la persona de la menor (y la atención psicológica no fuera consecuencia de la afectación por la violencia contra su madre) es aún más clara la irrelevancia de la mediación del progenitor. En ocasiones podrá haber tenido lugar la intervención judicial, del juzgado de violencia sobre la mujer, imponiendo medidas de protección respecto de la madre y la hija, medidas que eliminarán cualquier duda a este respecto.

En cuanto a la circunstancia de si con esa información se estaría revelando al progenitor la situación revelada por la madre, hay que descartarla por cuanto el progenitor ya será conocedor de que su pareja junto con su hija han abandonado el hogar, de modo que no se produce una quiebra de seguridad para la integridad de madre e hija.

FAQ 13

CUESTIÓN PLANTEADA: **¿Cómo afecta a la normativa de protección de datos la reciente entrada en vigor del instrumento de ratificación del Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra la mujer y la violencia doméstica, firmado en Estambul el 11 de mayo de 2011?**

El instrumento de ratificación del convenio era una cuestión pendiente desde hace más de 20 años, concretamente desde el año 1981 que es el año del Convenio 108 cuyo objeto es la protección de datos personales.

Por lo tanto, el instrumento de ratificación recientemente aprobado que entró en vigor el 1 de agosto de 2014 no supone ninguna reforma jurídica que el estado español no haya contenido en la LOPD, de modo tal que no aporta nada nuevo en materia de protección de datos personales, siendo así que expresamente se remite al Convenio 108 del Consejo de Europa antecitado de 28 de enero de 1981. De ese modo, se convierte en un instrumento de carácter vinculante en el ámbito europeo en esta materia y el tratado internacional de mayor alcance para hacer frente a la violencia contra las mujeres.

De hecho, el convenio recoge medidas ya consolidadas en el estado como la formación de los distintos colectivos de profesionales que intervienen en las situaciones de violencia contra las mujeres, el teléfono 016 facilitado por el Estado o el teléfono 900840101 en el ámbito del País Vasco, y un sistema de información estadística de datos relativos a violencia de género.

La novedad sí afecta a la introducción en el Código Penal de nuevos tipos penales; así el convenio contempla como delito todas las formas de violencia contra las mujeres: la violencia

física, psicológica y sexual, incluida la violación; la mutilación genital femenina, el matrimonio forzado, el acoso, el aborto forzado y la esterilización forzada. Ello implica que los estados deberán introducir en sus sistemas jurídicos estos delitos, que España ya incluye en su ordenamiento. De hecho, el matrimonio forzado, por ejemplo, se introduce como delito en el proyecto de Ley Orgánica de reforma del Código Penal, que está tramitándose en el Congreso.

Y en relación a la protección de datos, lo que supone, precisamente, es que Europa va a poner atención a que la normativa de protección de datos de carácter personal en los supuestos de violencia contra las mujeres se cumplan, designando para ello un grupo numeroso de personas.

Este escenario se verá reforzado con la próxima aprobación del Reglamento Europeo del que se anuncia que endurecerá las responsabilidades de las empresas y organizaciones públicas y privadas en el tratamiento de datos personales con las consiguientes declaraciones de infracción. Adapta la protección de datos a las nuevas demandas del mundo digital, ya que las actuales disposiciones se impusieron cuando en Europa menos del 1 % de la población utilizaba Internet, y se dirige a incrementar la confianza de las consumidoras y consumidores respecto del uso de su información personal.

3. CESIÓN DE DATOS PERSONALES

FAQ 14

CUESTIÓN PLANTEADA: **Se pregunta cómo garantizar la atención integral a todas las mujeres víctimas de violencia de género sin vulnerar los derechos que les reconoce la ley de protección de datos.**

Se indica que esta duda surge cuando las mujeres son derivadas por otros servicios de carácter diferente al municipal y el requisito para poder contactar con ellas es a través de sus datos de carácter personal.

Hay que diferenciar entre dos tipos de comunicaciones: la derivación y la cesión.

Por ejemplo, no sería lo mismo que la comunicación fuera desde los servicios sociales que, al darse cuenta de que una persona atendida es víctima de violencia de género, la reorienten a un servicio específico en esta materia (derivación), que aquel escenario en el que quien reorienta es cualquier otro servicio ajeno a los servicios sociales, que atiende a la mujer para otros fines, y teniendo conocimiento de que la mujer enfrenta violencia se ponga en contacto con los servicios sociales para que intervengan sin constar el consentimiento de la mujer (cesión).

En el primer caso, la finalidad de las atenciones que recibe la persona son similares, y se dirigen a abordar la misma finalidad, de modo que podríamos entender que la utilización de los datos inicialmente facilitados por la persona en vuestro servicio estaría amparada por el consentimiento inicial de la persona que facilitó al inicio de su intervención.

En el segundo, hay un cambio de finalidad de los datos, por lo tanto, no puede realizarse la comunicación de dichos datos sin el consentimiento de la víctima. En este caso, el servicio remitente debería comunicar a la persona la conveniencia de personarse y recibir asesoramiento y ayuda desde el servicio de igualdad y violencia, y que fuera la víctima la que acudiera voluntariamente.

También sería válido que el servicio remitente recogiera el consentimiento de la persona a que su información fuera remitida al servicio de igualdad y contra la violencia, enviando a continuación el expediente, acompañado de dicho consentimiento.

En cuanto a si quien remite puede o no guardar datos de la persona que ha remitido, esto se responde fácilmente, ya que sólo podrá guardar sus datos si va a continuar asistiendo o facilitando algún servicio a la persona; en cambio, si al remitirla al servicio de igualdad y violencia ha terminado su trabajo, en cuyo caso no podrá mantener ninguna información, debiendo proceder a la cancelación de los datos.

FAQ 15

CUESTIÓN PLANTEADA: **Mujer que acude a la Ertzaintza para denunciar en la comisaria el acoso que sufre por parte del padre de su novio y abuelo del hijo que tienen en común. En la comisaría le dicen que el abuelo en cuestión ya fue en su momento denunciado por su mujer por violencia de género. ¿esa información se la pueden dar? Lógicamente es muy interesante para la mujer y yo también la manejaba pero pensé que no podía decírselo al entender que me saltaba la ley de protección informándole de ello. ¿yo podría hacerlo?, ¿la policía puede hacerlo?**

La cuestión planteada es muy interesante y sobre todo el hecho de que se plantea desde una intuición sobre la ley de protección de datos que es muy correcta.

En efecto, cualquier revelación de datos que se haga por la organización que los tiene a persona distinta de la propia interesada es una cesión de datos, en términos legales.

Las cesiones de datos están prohibidas en el sistema de la Ley Orgánica de Protección de Datos, y sólo caben con el consentimiento de la persona titular de los datos o si existe una previsión en una norma de rango legal. En este caso, podemos presumir que no hay consentimiento del abuelo/suegro.

Así pues, esta actuación de revelación de datos no está permitida.

La única posibilidad que pudiera darse es que la policía le haya dado esta información con una finalidad de protección, de prevenirle de las posibles actuaciones futuras, pero para ello no hace falta concretar. Simplemente hubiera valido con advertirle expresamente de que tuviera una especial atención a comportamientos violentos, para que los denunciara, o haber adoptado alguna medida de protección de la víctima.

Así pues, la cesión no estaría justificada.

Ese dato puede ser útil que lo tengas para poner en contexto la situación y adoptar medidas de protección/ayuda más adecuadas, pero hay que considerar tu reacción correcta, no puedes ceder ese dato que recogiste en su día en el marco de otra asistencia distinta. En todo caso, tendrías que tener antes el consentimiento del abuelo/suegro o de la víctima, su mujer, para poder ceder el dato.

FAQ 16

CUESTIÓN PLANTEADA: **Tenemos la duda de si la información que recogemos al atender a una víctima de violencia puede ser compartida entre diferentes departamentos del propio ayuntamiento sin la autorización expresa de la víctima. Concretamente la información se transmite entre los departamentos de Servicios Sociales, Policía Municipal e Igualdad.**

La cuestión planteada apunta a uno de los aspectos más problemáticos que se plantean en el ámbito de la protección de datos relacionada con la violencia contra las mujeres en el entorno municipal.

Algunas cuestiones como punto de partida.

Inicialmente, puntualizamos en la guía que el momento de la recogida y de proporcionar la debida información a la víctima es esencial, ya que determina de forma relevante el futuro del uso de la información por la Administración. En este momento de la recogida, se debe precisar de forma clara su finalidad, siendo recogida la información estrictamente indispensable para el fin que se persigue. En este caso, se recoge la información imprescindible para la finalidad de asistir, ayudar o asesorar a la víctima, en su caso para presentarse a una solicitud de ayudas si fuera ése el escenario a modo de ejemplo.

Lo primero, por lo tanto, es determinar que la recogida de información se hace exclusivamente para conseguir una finalidad. Esta información que ha sido recogida, la deberán de tratar o utilizar, siempre para conseguir esa finalidad, algunos de los servicios municipales, entre ellos las personas encargadas y funcionarios y funcionarias de los servicios sociales. Y puede

ser que también el Departamento municipal competente en materia de vivienda social debe conocerlos para incluir, por ejemplo, a la mujer víctima de violencia en las listas de beneficiarias de viviendas reservadas a este colectivo.

Así pues, y siempre dentro de la finalidad perseguida, puede ser que haya otros departamentos que conocerán los datos para ese fin. Pero no debemos olvidar que deberán conocer sólo y exclusivamente aquellos datos personales de la víctima que sean útiles para esa finalidad.

A modo de ejemplo, el departamento competente en materia de vivienda no podrá ver los partes de lesiones o historia clínica si ésta se encuentra en poder del departamento de asuntos sociales, porque no lo necesita para el ejercicio de su competencia.

En este entorno es en el que debemos enmarcar la respuesta.

Además, hay que indicar que la recogida de información por el ayuntamiento siempre se hará con esta idea, y siempre con el consentimiento de la víctima.

Si se considerara necesario que haya una compartición absoluta de la información correspondiente a la víctima en el ámbito municipal, y esta compartición se pudiera justificar, siempre es recomendable que la mujer víctima lo conozca y sea solicitado su consentimiento.

Tampoco hay que olvidar que toda actuación municipal se rige por el ejercicio de unas competencias establecidas en una norma jurídica. El departamento competente en materia de servicios sociales así lo estará haciendo, y dentro del ejercicio de esas competencias, se debe atener a la ley.

Así pues, y contestando a la cuestión planteada, en relación a si pueden cederse los datos entre distintos servicios municipales, la respuesta debe ser negativa, salvo en el caso de que tenga como finalidad el ejercicio de competencias municipales relacionadas con la atención a una víctima de violencia.

En el caso planteado, si se pueden ceder los datos entre los departamentos de servicios sociales, policía municipal e igualdad, la respuesta nos vendrá dada por lo anteriormente expuesto.

Tampoco va a tener la misma solución en el caso de que los datos se hayan recogido por unos u otros de los servicios expuestos.

En la cuestión planteada, y siguiendo un esquema binario (de uno a uno), existen seis posibles cesiones en función de quién es la parte cedente (la que entrega) y quién es la parte cesionaria de la información (la que la recibe).

Atendiendo al planteamiento de la cuestión, las distintas posibilidades de cesión son:

— Datos recogidos por servicios sociales enviados al departamento competente en igualdad.

— Datos recogidos por servicios sociales enviados a la policía municipal.

— Datos recogidos por la policía municipal enviados al departamento de servicios sociales.

— Datos recogidos por la policía municipal enviados al departamento de igualdad.

— Datos recogidos por el departamento de igualdad enviados a la policía municipal.

— Datos recogidos por el departamento de igualdad enviados a servicios sociales.

Cada una de las opciones mencionadas se debe analizar como una posible cesión de datos personales.

En principio, y con carácter general, debe responderse que la información cedida a la policía municipal, siempre que se dirija en el marco de la investigación de un hecho delictivo o en colaboración con otras policías para ese fin, o para la prevención del delito, está amparada por la Ley de Enjuiciamiento Criminal y el Código Penal.

El resto de cesiones previstas, siempre que se hagan dentro de los servicios municipales de servicios sociales o con la finalidad de coadyuvar a la atención a la víctima con una misma finalidad, no plantean problemas, y podrían hacerse.

Plantean a priori más problemas las cesiones de datos que tenga la policía municipal en el marco de las investigaciones policiales. Estos datos, recogidos y tratados en el marco de estas investigaciones policiales no podrán ser cedidos a los servicios sociales municipales dado que se recogieron y se están tratando con esa finalidad. Estos datos, en principio y generalmente considerados, no podrán ser cedidos a los servicios sociales o departamento de igualdad.

FAQ 17

CUESTIÓN PLANTEADA: **En ocasiones a las mujeres víctimas de violencia y atendidas por el Juzgado se les deriva al SAV (Servicio de Atención a la Victima) que se encuentra en Donostia en el caso de Gipuzkoa, por lo que se tienen que desplazar a esa localidad. Posteriormente, tras su atención en el SAV, hay situaciones en las que las mujeres requieren atención o gestión de determinados recursos (prestaciones económicas, atención psicológica, etc.) y las mujeres tienen que acudir a estos servicios municipales. A veces ello provoca trastornos y pérdida de tiempo en la gestión de recursos.**

En este mismo sentido, detectamos que por parte del Juzgado en algunos casos no se orienta a la víctima a que pueda acercarse a los servicios sociales municipales para plantear su situación de necesidad. Sobre todo en las ocasiones en que existe Orden de Protección, esto sería conveniente (a veces las mujeres víctimas acuden a los servicios sociales de mutuo propio, pero cuando ya ha pasado bastante tiempo desde que ha ocurrido la situación de violencia).

En relación a las prestaciones económicas para mujeres víctimas a conceder desde el GV, en ocasiones se exige documentación que inicialmente no está en la relación de documentos a aportar junto a la solicitud. Ayudaría el aclarar y saber de antemano en qué situaciones o circunstancias es necesario aportar otro tipo de documentación.

En la gestión de estas últimas ayudas, desde GV en ocasiones se requiere al ayuntamiento aportar documentación para resolver el expediente, por lo que la trabajadora social se tiene que poner en contacto con la interesada para comunicarle la documentación requerida, y a veces con dificultades por parte de la profesional para responder sus dudas. Consideramos más conveniente, rápido y efectivo que se requiera la documentación directamente a la interesada.

Efectivamente, el gran problema que se plantea en la protección de datos es el de la existencia de múltiples intervinientes en el ámbito de la protección de las mujeres víctimas de violencia.

Desde la protección de los datos personales hay que decir, con carácter general, que la recogida de la información por cada interviniente en el proceso de asistencia a las víctimas se tiene que regir por el principio de calidad, es decir, limitándose a la finalidad de la asistencia. Así, el juzgado sólo podrá recabar los datos necesarios para la finalidad de la persecución del delito, y el ayuntamiento o el servicio de asistencia a la víctima, sólo los datos relacionados con su función.

Por lo que respecta a la cesión o comunicación de datos a terceras personas físicas o jurídicas, el intercambio de datos personales entre los distintos intervinientes en el proceso de asistencia no puede realizarse si no es con el consentimiento de la víctima, que es la propietaria de los datos, o que exista una habilitación expresa en una norma con rango legal, como sucede con la obligación de comunicar a la policía o al juzgado hechos delictivos, fundamento que reside en la investigación del delito. Hay que advertir que una norma con rango legal no es un convenio de colaboración o de coordinación interinstitucional.

Por lo tanto, tanto la intervención de los servicios municipales como la del Gobierno Vasco, si se prevé el intercambio de información, puede realizarse, actualmente y en principio, sólo con este consentimiento, de la mujer víctima de violencia.

No hay ningún problema en que unos u otros aconsejen a la víctima que se dirija a otro servicio, mientras no haya cesión de documentación o datos personales entre ellos.

En cuanto a si la solicitud de documentación debe realizarse por el Gobierno Vasco al ayuntamiento o a la víctima, lo importante es que en todo caso sea la víctima la que dé su consentimiento para que vosotros y vosotras enviéis esa documentación. Es decir, desde la protección de datos es irrelevante que lo enviéis o que se solicite directamente a la víctima, mientras en todo caso medie el consentimiento de ésta.

FAQ 18

CUESTIÓN PLANTEADA: **Una chica se pone en contacto con Emakunde y nos escribe un e-mail quejándose de la atención recibida en uno de los servicios del gobierno a mujeres víctimas de violencia. Emakunde, que coordina el II Acuerdo, le responde que va a trasladar la queja a la entidad correspondiente. ¿Necesitamos recoger la autorización de la cesión de datos o entendemos que la recepción de la queja presupone/autoriza ya ese traslado?**

En primer lugar, habría que conocer de qué tipo de queja se trata, por cuanto no es lo mismo manifestar la contrariedad por el trato o la atención recibida que manifestar la disconformidad con la no concesión de una ayuda o servicio.

En el primer caso, para trasladar la queja no se necesita conocer los datos personales de la persona. Máxime si se trata de una mujer víctima de violencia la que expone la queja. Bastaría con disociar los datos; esto es, eliminar los datos de identidad, domicilio, etc. y remitir la queja, de esa manera, a la entidad correspondiente. De ese modo, si se considera necesario comunicar su resultado a la reclamante, Emakunde dispone de la totalidad de los datos de esa persona para comunicarse con ella y trasladarle el resultado de la queja.

Sin embargo, si la entidad se limita a reconducir la queja, sin guardar ninguna información, ni el correo electrónico, ni su contenido, de la persona remitente, se ha producido únicamente una actuación puntual, y no estamos ante una cesión. Cuestión distinta al escenario que se indica a continuación.

En el segundo escenario, el servicio correspondiente tendrá todos los datos de identidad de esa persona. Sin embargo, y para mayor cautela, sería conveniente recoger el consentimiento de la solicitante para remitir la queja al Departamento del Gobierno competente. De ese modo, sería conveniente en los formularios de queja incluir la previsión de recogida de consentimiento para estos supuestos. Ello vuelve a colocarnos en la necesidad de un enfoque global de la seguridad de la información y protección de datos de carácter personal.

4. LA SEGURIDAD DE LOS DATOS PERSONALES

FAQ 19

CUESTIÓN PLANTEADA: **¿Quién puede tener acceso a la información sobre los casos de mujeres víctimas de violencia de género?, ¿todas las personas que se encuentran dentro del protocolo o puede tener acceso alguien más?**

Cuando se recogen datos de una víctima, esta recogida se hace con una finalidad determinada y única. En este caso, el realizar la asistencia y ayuda a la víctima en todos los ámbitos sociales.

Esa recogida de datos se debe hacer informando a la víctima de qué uso se va a dar a sus datos y a la información que presta a la administración.

No es posible, sin su conocimiento y su consentimiento, que esa información se utilice para otros fines, sean los que sean. Sin ese consentimiento, una primera posibilidad que se abre para que los datos que la víctima ha prestado a la administración sean cedidos a otras personas o administraciones es que haya una norma de rango legal que prevea dicha cesión; así ocurre en el caso de la cesión de datos a la policía, que se encuentra prevista en el artículo 22. 2 y 3 LOPD, que prevé la recogida y comunicación a la policía de datos de carácter personal aun sin consentimiento de la persona titular cuando la recogida tenga por objeto la prevención de un peligro o la represión de infracciones penales. La segunda posibilidad es la cesión de datos entre organismos o entidades de la administración con competencias sobre la misma materia y que se encuentra contemplado en el art. 21 LOPD.

La existencia de protocolos en el ámbito municipal no habilita la cesión de datos entre quienes participan en el mismo. Es decir, no es suficiente con que haya un protocolo como

amparo legal para la cesión. En todo caso, sin consentimiento o amparo en una norma de rango legal no se pueden ceder los datos.

La utilidad de los protocolos reside en la definición de mecanismos de colaboración y ayuda, pero debe ser la propia víctima la que defina y autorice a quién se van a ceder dichos datos.

Así pues, deberías recoger previamente su consentimiento para la cesión, y además el consentimiento para cesiones concretas y no genéricas, definiendo con claridad a quién se va a ceder dichos datos para que la víctima lo conozca sin ninguna duda.

FAQ 20

CUESTIÓN PLANTEADA: **Una entidad tiene recogidos adecuadamente los datos personales de una mujer que enfrenta violencia y piensa que le puede ser de ayuda que la mujer sea atendida por los servicios sociales de base. Le pide el consentimiento para ello a la mujer y esta acepta. Sin embargo, la entidad conoce que en los servicios sociales de ese ayuntamiento no se respetan adecuadamente las medidas del nivel de protección alto que esa información merece. ¿Sobre quién recaería la responsabilidad en caso de que la entidad finalmente cediera los datos a los servicios sociales?, ¿los debería ceder?**

Si conoce que los servicios de base a los que se van a ceder los datos personales carecen de las medidas de seguridad adecuadas, no debería ceder esos datos.

Para evitar responsabilidades de unas u otras entidades o servicios debe contenerse en los protocolos de actuación la previsión de cumplimiento de las medidas de seguridad de nivel alto de la LOPD por todos los órganos y entidades participantes en dicho protocolo.

ANEXO 3: LA CESIÓN DE DATOS EN LA ATENCIÓN A LAS PERSONAS MENORES DE EDAD ANTE SITUACIONES DE VIOLENCIA CONTRA LAS MUJERES

1. NORMATIVA PARA LA PROTECCIÓN DE LOS Y LAS MENORES DE EDAD

Se ha planteado con motivo de la elaboración de esta guía que la supremacía del interés del menor o de la menor ha de ser un principio rector de la actuación administrativa del art. 11 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor. BOE 17/enero/1996).

Se indica que, específicamente, en nuestra Comunidad Autónoma está regulado que "las administraciones públicas, en el ámbito de sus competencias, ejercerán la protección social y jurídica de los niños, niñas y adolescentes, atendiendo a los siguientes principios: a) Se respetará, en todas las actuaciones, el principio de primacía del interés superior de los niños, niñas y adolescentes y la protección de sus derechos en orden a garantizar su desarrollo sobre cualquier otro interés legítimo concurrente (...)" (art. 48 de la Ley 3/2005 del 18 de febrero de Atención y Protección a la Infancia y la Adolescencia. BOPV 30/marzo/2005).

Además, "las autoridades y los servicios públicos tienen obligación de prestar la atención inmediata que precise cualquier menor, de actuar si corresponde a su ámbito de competencias, o de dar traslado en otro caso al órgano competente y de poner los hechos en conocimiento de los representantes legales del menor, o cuando sea necesario, del Ministerio Fiscal." (art. 14 Ley Orgánica 1/1996). Por su parte, "los titulares de los centros educativos y el personal de los mismos están obligados a poner en conocimiento de las administraciones públicas competentes en materia de protección de personas menores de edad, o cuando sea necesario del ministerio fiscal o de la autoridad judicial, aquellos hechos que puedan suponer malos tratos o la existencia de desprotección o riesgo infantil, debiendo comunicar los datos e informaciones que resulten necesarios y suficientes para garantizar la calidad y la eficacia de las intervenciones, así como colaborar con las citadas administraciones para evitar y resolver estas situaciones, si bien deberán tenerse siempre en cuenta los intereses prioritarios de las personas menores de edad". (art. 25.2 de la Ley 3/2005 del 18 de febrero de Atención y Protección a la Infancia y la Adolescencia. BOPV 30/marzo/2005).

Más concretamente, en el procedimiento ordinario seguido por los servicios sociales en situaciones de desamparo de una persona menor de edad la normativa dispone que: "En el momento en que la administración pública competente en materia de protección de menores tenga conocimiento de que un niño, niña o adolescente puede encontrarse en situación de desamparo, debe iniciar un expediente cuya tramitación responderá a las siguientes pautas de

actuación: a) Solicitar informes a cuantas personas u organismos puedan facilitar datos relevantes para el conocimiento y la valoración de la situación sociofamiliar, especialmente a los servicios sociales de base. Si se estima necesario, se solicitarán informes al tutor escolar y al médico de familia o al pediatra, o a cualquier otro profesional de la salud u otros ámbitos de atención social o educativa, debiendo estos profesionales transmitir por escrito los datos e informaciones necesarias y suficientes de los que dispongan para garantizar la calidad y la eficacia de las intervenciones. b) Informar a los organismos y profesionales que colaboren en la detección y valoración de una situación de riesgo o desprotección de las líneas generales de su evolución, dentro de los límites exigidos por el deber de reserva y siempre que no resulte improcedente dicha comunicación (...)". (art. 58.1 Ley 3/2005)

2. INTERPRETACIÓN DE LA NORMATIVA PARA LA PROTECCIÓN DE LOS Y LAS MENORES DE EDAD EN RELACIÓN A LA LEY ORGÁNICA PARA LA PROTECCIÓN DE DATOS PERSONALES

Sentado este planteamiento jurídico, ¿podemos concluir que las previsiones normativas antes citadas suponen suficiente título habilitante para las cesiones de datos concretos?

Con carácter general, hay que reiterar que las cesiones tienen como regla general el consentimiento, y ésta ha sido, y debe ser, la recomendación más importante en la materia. En efecto, recoger el consentimiento de la víctima o de los terceros cuyos datos se van a tratar es la piedra angular sobre la que reposan nuestras consideraciones. Sin embargo, como también hemos indicado, es posible que las cesiones de datos tengan una habilitación legal, es decir, haya una norma de rango legal que habilite la cesión. Dicha norma debe ser expresa, y no genérica, y supone un análisis de su redacción para poder concluir si, en efecto, es o no título suficiente.

Analizando la posible existencia de habilitación legal para la cesión en este escenario concreto, procede efectuar las siguientes consideraciones:

Primera: Inicialmente se plantea la existencia de un "principio rector de la actuación administrativa (art. 11 de la Ley Orgánica 1/1996 de 15 de enero de Protección Jurídica del Menor. BOE 17/enero/1996)". Más específicamente, la regulación de nuestra Comunidad Autónoma dice que "las administraciones públicas, en el ámbito de sus competencias, ejercerán la protección social y jurídica de los niños, niñas y adolescentes, atendiendo a los siguientes principios: a) Se respetará, en todas las actuaciones, el principio de primacía del interés superior de los niños, niñas y adolescentes y la protección de sus derechos en orden a garantizar su desarrollo sobre cualquier otro interés legítimo concurrente (...)" (art. 48 de la Ley 3/2005 del 18 de febrero de Atención y Protección a la Infancia y la Adolescencia. BOPV 30/marzo/2005)

Analizando hasta aquí la previsión normativa, en efecto se concreta la existencia de un principio rector que pone en valor como principio esencial la primacía del interés del menor o de la menor de edad.

Sin embargo, no deja de ser un principio general de actuación administrativa, pero que no tiene una remisión directa a la autorización a la administración a ceder los datos de los y las menores de edad siempre, y en todo caso, que se encuentre una situación que requiera dicha actuación de protección social de los niños y las niñas. Asistimos a un conflicto de derechos, ya que la ley orgánica de protección de datos, que desarrolla un derecho constitucional, no contiene previsión al respecto.

Segunda: Se recoge a continuación la mención del artículo 14 de la Ley Orgánica 1/1996, de Protección Jurídica del Menor de la misma ley, según el cual "Las autoridades y los servicios públicos tienen obligación de prestar la atención inmediata que precise cualquier menor, de actuar si corresponde a su ámbito de competencias, o de dar traslado en otro caso al órgano competente y de poner los hechos en conocimiento de los representantes legales del menor, o cuando sea necesario, del Ministerio Fiscal".

Nuevamente, hay una previsión sobre la obligación de poner en conocimiento estas situaciones, prestar atención inmediata, etc. Sin embargo, el artículo 14 de la Ley Orgánica 1/1996, de Protección Jurídica del Menor recoge cuatro obligaciones o situaciones:

1) Que las autoridades deban prestar la atención inmediata que precise cualquier menor, no contiene ninguna previsión de cara a la cesión, sino que establece una obligación de intervención para cada administración.

2) Que la obligación de actuar si corresponde a su ámbito de competencias, tampoco tiene ninguna relación con las cesiones, sino más bien constituye una limitación a la actuación administrativa para evitar actuaciones al margen de sus competencias.

3) Dar traslado al órgano competente prevé que si hay conocimiento de los hechos y no hay competencia para actuar, se dé traslado al órgano competente. En este caso, podríamos entrever una habilitación.

   En efecto, se trata de una situación en la que un órgano detecta que un o una menor requeriría intervención, pero no se puede actuar por falta de competencias; en este caso, se debería dar traslado al órgano competente en infancia o atención a las personas menores de edad.

   Esto es, una entidad que tiene como actividad la atención social detecta una situación que requiere actuación inmediata a una persona menor de edad y no es competente para ello por la especificidad de la atención en estos escenarios. En ese caso, el organismo o enti-

dad de servicios sociales que tiene conocimiento de la situación debe comunicar los datos al organismo o entidad competente en materia de atención a la infancia.

Sin embargo, analizado detalladamente, vemos que esta previsión tiene dos límites: primero, sólo se podrá actuar en casos de situaciones en que el o la menor precisa atención INMEDIATA, relacionado claramente con la urgencia; y segundo, sólo se puede poner en conocimiento de un servicio que tenga competencias sobre la materia asistencial a la persona menor de edad.

4) La cuarta previsión del artículo 14 de la Ley Orgánica 1/96 es la cesión de esa información sobre la necesidad de intervención ("poner los hechos en conocimiento") de los y las representantes legales del o la menor de edad, cuestión que habilitaría solo a comunicarlo a padres y madres o a quienes tengan la tutoría legal, y en segundo caso, y con la limitación de "cuando sea necesario", al Ministerio Fiscal. Los supuestos de puesta en conocimiento del Ministerio Fiscal se encuentran regulados en la ley (Código Civil, Código Penal, y legislaciones procesales), y básicamente van dirigidos a la actuación del Ministerio Fiscal en el ámbito judicial, utilizando herramientas procesales para la defensa del interés del o la menor de edad. Estas cesiones tampoco plantean problemas ya que la actuación del Ministerio Fiscal será normalmente a petición de la propia administración en casos relacionados con el ámbito penal prioritariamente.

Tercera: En relación con las cesiones desde los centros educativos, el artículo 25.2 de la Ley 3/2005 del 18 de febrero de Atención y Protección a la Infancia y la Adolescencia (BOPV 30/marzo/2005) dice: "Los titulares de los centros educativos y el personal de los mismos están obligados a poner en conocimiento de las administraciones públicas competentes en materia de protección de personas menores de edad, o cuando sea necesario del ministerio fiscal o de la autoridad judicial, aquellos hechos que puedan suponer malos tratos o la existencia de desprotección o riesgo infantil, debiendo comunicar los datos e informaciones que resulten necesarios y suficientes para garantizar la calidad y la eficacia de las intervenciones, así como colaborar con las citadas administraciones para evitar y resolver estas situaciones, si bien deberán tenerse siempre en cuenta los intereses prioritarios de las personas menores de edad".

En efecto, las y los educadores y quienes son responsables de los centros educativos, tienen la facultad de poner en conocimiento situaciones o hechos que impliquen la necesidad de asistencia social. Sin embargo, en el artículo mencionado no se habilita a una cesión de datos con carácter general, sino a poner en conocimiento que se está produciendo una situación que precisa intervención. Ello no habilita a la cesión de cualquier otro tipo de dato que el centro educativo haya recogido en el ejercicio de sus competencias educativas.

Así, la elaboración de informes o comunicación de información que sea necesaria para la atención social debe entenderse en todo caso de forma restringida y restrictiva, debiendo ceder, en su caso, y a petición de las administraciones que intervengan la información estrictamente necesaria.

Entendemos que una intervención social posterior que requiera la incorporación, por ejemplo, de informes internos del colegio, expediente académico u otras cuestiones, sólo se puede producir con el consentimiento de la o del menor (+14 años) o de sus madres, padres o personas tutoras (-14 años), ya que no se encuentra habilitada la cesión en este artículo.

Cuarta: Por último, se menciona la previsión del artículo 58.1 de la Ley 3/2005; esta previsión normativa va dirigida y se encuentra restringida a las situaciones de desamparo, y no a toda intervención social para la protección del o la menor de edad.

Se define el desamparo en la propia ley en su artículo 56 como: "(…) la que se produce de hecho a causa del incumplimiento, o del imposible o inadecuado ejercicio de los deberes de protección establecidos por las leyes para la guarda de las personas menores de edad, cuando éstas queden privadas de la necesaria asistencia moral o material".

Es decir, las situaciones de intervención social que requieren la asunción de la tutela de los y las menores de edad por la administración pública, por graves situaciones de desamparo.

La concreción de las distintas situaciones en las que puede encontrarse un o una menor de edad se encuentran reguladas en el Decreto 230/2011, de 8 de noviembre, por el que se aprueba el instrumento para la valoración de la gravedad de las situaciones de riesgo en los servicios sociales municipales y territoriales de atención y protección a la infancia y adolescencia en la Comunidad Autónoma del País Vasco (BALORA). Por lo tanto, dejemos sentado inicialmente que se trata de un tipo de intervención social muy concreta y la más grave, ya que priva a los o las progenitoras de la guarda y custodia de las personas menores de edad.

Sentadas las bases, analicemos la previsión del artículo 58.1 de la Ley 3/2005, de Atención y Protección a la Infancia y la Adolescencia:

"En el momento en que la administración pública competente en materia de protección de menores tenga conocimiento de que un niño, niña o adolescente puede encontrarse en situación de desamparo, debe iniciar un expediente cuya tramitación responderá a las siguientes pautas de actuación: a) Solicitar informes a cuantas personas u organismos puedan facilitar datos relevantes para el conocimiento y la valoración de la situación sociofamiliar, especialmente a los servicios sociales de base. Si se estima necesario, se solicitarán informes al tutor escolar y al médico de familia o al pediatra, o a cualquier otro profesional de la salud u otros ámbitos de atención social o educativa, debiendo estos profesionales transmitir por escrito los datos e informaciones necesarias y suficientes de los que dispongan para garantizar la calidad y la eficacia de las intervenciones. b) Informar a los organismos y profesionales que colaboren en la detección y valoración de una situación de riesgo o desprotección de las líneas generales de su evolución, dentro de los límites exigidos por el deber de reserva y siempre que no resulte improcedente dicha comunicación (...)".

Por tanto, el apartado a) del artículo 58.1 de la Ley 3/2005 de Atención y Protección a la Infancia y la Adolescencia, habilita la petición de información: primero, "a cuantas personas u organismos puedan facilitar datos relevantes" y, segundo, siempre con una finalidad, que es conocer y valorar la situación sociofamiliar. En este caso, entendiendo que se produzca una situación de desamparo vinculada a un episodio o situación de violencia, entendemos que la administración competente podrá solicitar dichos informes. Pero no deberá solicitarse la cesión del expediente completo sino de lo estrictamente necesario para valorar la situación socio familiar, y mediante la realización de un informe ad hoc para ello.

Sólo si se estima necesario, podrán solicitarse informes al tutor o tutora, al médico o la médica de familia o pediatra.

Es importante destacar en este caso que existe una obligación de transmitir la información por escrito, pero también es importante apreciar la propia autolimitación en la transmisión de esta información, ya que se habla de informaciones "necesarias y suficientes" para "garantizar la calidad y eficacia de las intervenciones". No se menciona quién debe valorar esta finalidad y el cumplimiento de esta autolimitación, pero entendemos que serán ambas partes, tanto la persona cedente como la cesionaria.

3. RESUMEN: LOS Y LAS MENORES DE EDAD Y LA PROTECCIÓN DE DATOS

A modo de conclusión, analizada la normativa antes citada, podemos establecer las siguientes consideraciones:

1. La existencia de un principio rector de la actuación administrativa en beneficio del o la menor de edad no constituye en nuestra opinión título legal habilitante para la cesión de datos relativos a personas menores de edad entre las administraciones públicas.

2. La redacción del artículo 25.2 de la Ley 3/2005 del 18 de febrero de Atención y Protección a la Infancia y la Adolescencia habilita exclusivamente las cesiones entre administraciones públicas con dos límites: primero, sólo se podrá actuar en casos en que el menor o la menor precisa atención INMEDIATA, relacionado claramente con la urgencia; y segundo, se podrá poner en conocimiento por un servicio que tiene como competencia la atención social a otro idéntico, que por competencia sea el que debe intervenir. Asimismo, prevé las cesiones al Ministerio Fiscal, que ya están reguladas en las normas que prevén las competencias de éste, y que fundamentalmente van dirigidas a la persecución de la comisión de un hecho delictivo.

3. El artículo 25.2 de la Ley 3/2005 del 18 de febrero de Atención y Protección a la Infancia y la Adolescencia no habilita la cesión de datos desde los centros educativos a otras administraciones públicas, sino a poner en conocimiento hechos o circunstancias observadas

o conocidas por el personal educativo, y por lo tanto, dentro de las obligaciones genéricas de la normativa.

4. Constituye un título legal habilitante para la cesión de datos de menores en situación de desamparo la previsión del artículo 58.1 de la Ley 3/2005 del 18 de febrero de Atención y Protección a la Infancia y la Adolescencia, con los siguientes límites: primero, afecta sólo a supuestos de desamparo y a partir de que la administración conozca esta situación; segundo, no habilita a la cesión de expedientes íntegros, sino a la elaboración de informes que puntualmente y sólo en la medida en que sea imprescindible pueden contener datos o informaciones en poder de otras administraciones públicas; tercero, debe tenerse en cuenta en todo momento la aplicación del principio de calidad, especialmente recogido en el artículo 58.1, que indica que sólo se podrán ceder aquellos datos estrictamente necesarios para la finalidad perseguida y, por lo tanto, a órganos con competencia en la materia.