Preguntas frecuentes en relación con la Protección y el tratamiento de los datos de carácter personal en la actual crisis sanitaria provocada por el virus Covid-19.

Grupo Técnico de trabajo sobre Protección de Datos

Comisión de Sociedad de la Información, Innovación Tecnológica y Agenda Digital

Federación Española de Municipios y Provincias.

Integrantes del Grupo de Trabajo

Técnicos de la Comisión:

- **Ascen Moro Cordero**, Delegada de Protección de Datos, Ayuntamiento de Sant Feliu de Llobregat
- **Concepción Campos Acuña**, Secretaria del Gobierno Local, Ayuntamiento de Vigo
- **Lluís Sanz Marco**, Delegado de Protección de Datos, Ayuntamiento de Barcelona
- **Virginia Moreno Bonilla**, Dirección General de NNTT e Innovación, Ayuntamiento de Leganés

Colaboradores externos:

- **Ana Marzo Portera,** Directora, Equipo Marzo
- **Miguel Ángel Lubian Rueda**, Socio-Responsable Área de Compliance, Instituto CIES
- **Ricard Martínez Martínez,** Director de la Cátedra de Privacidad y Transformación Digital Microsoft, Universitat de Valencia.

Coordinación FEMP:

- **Pablo María Bárcenas Gutiérrez**; Secretario de la Comisión de Sociedad de la Información, Innovación Tecnológica y Agenda Digital.

Introducción

La situación de emergencia de salud pública ocasionada por el COVID-19 ha requerido de la puesta en marcha de muchas medidas a escala nacional, comunitaria y local algunas de las cuales están requiriendo, en particular, el tratamiento de datos de carácter personal de la ciudadanía y el uso de tecnologías con un impacto fuera de lo habitual.

Desde la Federación Española de Municipios y Provincias (FEMP) se pone a disposición de las entidades locales información de ayuda y apoyo en relación con el tratamiento de los datos personales que se puedan estar llevando a cabo por las entidades locales para paliar los efectos contra el COVID-19.

Preguntas y respuestas:

1. **¿Hay alguna excepción de aplicación de la normativa de protección de datos durante la pandemia o como consecuencia del tratamiento de datos con fines de gestión de la pandemia?**

No. Tanto el Reglamento General de Protección de Datos (RGPD) como la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) son de aplicación a cualquier actividad de tratamiento de datos personales que lleve a cabo una entidad local como consecuencia del tratamiento de datos con fines de gestión de la pandemia.

Además, las entidades locales deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de acuerdo con lo previsto en el Esquema Nacional de Seguridad (ENS).

2. ¿Se puede crear una base de datos de personas vulnerables en la ciudad, que permita a los servicios sociales en coordinación con nuestra Agencia de Salud Pública, cubrir aspectos críticos durante la epidemia?

Sí. Nada impide desarrollar actividades legítimas necesarias ni hay obstáculo, pero siempre que se asegure que los datos son tratados en cada caso con pleno respeto al RGPD y a la LOPDGDD.

Si bien se tendrá que tener en cuenta el nuevo marco legal introducido por el decreto de declaración del estado de alarma, a partir de los criterios introducidos de forma específica para esta pandemia por el "statement de la EDPB" y especialmente, por el informe 0017/2020 del gabinete jurídico de la AEPD.

Es importante en todo caso que en el registro de actividades de la entidad local se genere un nuevo registro por cada nueva actividad de tratamiento que sea creada (en el que constará la información establecida en el artículo 30 del RGPD y su base legal) y que dicha actividad de tratamiento sea pública y accesible por medios electrónicos para las personas interesadas.

3. ¿Qué significa asegurar que los datos sean tratados con pleno respeto del RGPD y la LOPDGDD?

Significa que la base de datos cumpla los principios básicos de protección de datos y todas las garantías que se establecen para las personas físicas titulares de los datos, como son:

- Con carácter previo se analizará la necesidad de una evaluación de impacto según los criterios de la AEPD . En cualquier caso, aunque no exista la necesidad de evaluación de impacto siempre deberá llevarse a cabo un análisis de riesgos que permita la correcta aplicación de las políticas de seguridad.
- Aplicar el principio de privacidad desde el diseño a la cantidad de datos, a la extensión de su tratamiento, a su accesibilidad y a su plazo de conservación.
- Analizar la base jurídica aplicable y determinar los fines legítimos de tratamiento, los posibles destinatarios y la duración del tratamiento.
- Informar a las personas interesadas cuyos datos son objeto de tratamiento, informando la información a formularios, políticas de privacidad, locuciones telefónicas, envíos postales, u otras formas como enlace a la actividad de tratamiento.
- Aplicar las medidas de seguridad. En este sentido, se dispondrá como marco de referencia las políticas de seguridad corporativas que se hayan establecido para esta situación de emergencia específica que como mínimo garantice los principios de accesibilidad y integridad principalmente soportados sobre servidores corporativos de bases de datos o de ficheros (en cuyo caso debería optarse por la encriptación de estos). Sin perjuicio de que el marco general de cumplimiento para todas las Entidades locales lo marcan las medidas de seguridad definidas en el Anexo II del Esquema Nacional de Seguridad (ENS), así como aquellas medidas resultantes del análisis de riesgos). En todo caso, el mínimo de las medidas a establecer viene constituido por lo establecido en el artículo 32 del RGPD que exige medidas apropiadas como:
    - a) la seudonimización y el cifrado de datos personales;
    - b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
    - c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
    - d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
- Garantizar en plazo y contenido el ejercicio de los derechos de las personas.

Además, aunque el tratamiento sea novedoso y temporal debería quedar bajo el amparo de las políticas y procedimientos de protección de datos de la entidad local.

4. ¿Quién debe validar las medidas indicadas en el punto anterior?

La validación de las medidas indicadas en el punto anterior debería ser realizada por el delegado de protección de datos de la entidad local, sin perjuicio de las figuras definidas en los comités de seguridad: responsable de seguridad y responsable del sistema.

5. ¿Cuáles podrían ser las bases jurídicas de los nuevos tratamientos que se generen como consecuencia del COVID-19?

El RGPD contiene las salvaguardas y reglas necesarias para permitir legítimamente los tratamientos de datos personales en situaciones, como la presente, en que existe una emergencia sanitaria de alcance general y para estas situaciones el RGPD reconoce que la base jurídica de los tratamientos puede ser múltiple.

Los tratamientos datos personales encuentran en el artículo 6 distintas bases jurídicas legitimadoras, entre otras:
▪ el cumplimiento de una obligación legal;
▪ proteger intereses vitales del interesado o de otra persona física;
▪ cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

También podrán tratarse categorías especiales de datos de acuerdo con el artículo 9 RGPD cuando el tratamiento sea necesario:
▪ para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito de la seguridad y protección social;
▪ para proteger intereses vitales del interesado o de otra persona física;
▪ por razones de un interés público esencial;
▪ para la prestación de asistencia o tratamiento de tipo sanitario o social;
▪ por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud;
▪ en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento y el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

Debemos tener en cuenta que cada una de estas bases jurídicas deben encontrar reconocimiento expreso en la legislación interna y requieren adoptar las debidas cautelas y garantías adecuadas.

Informe AEPD

6. ¿Cuáles podrían ser los fines de los nuevos tratamientos que se generen como consecuencia del COVID-19?

El desarrollo de políticas públicas de asistencia social en coordinación con los servicios de salud pública y de control de la crisis sanitaria, como por ejemplo:

- El suministro de alimentos cocinados compras básicas de alimentación o medicamentos a gente mayor o personas en situación de vulnerabilidad;
- Atención a menores;
- Localizar posibles casos de masificación residencial, que puedan constituir un riesgo importante para los residentes y contactos vecinales;
- Cualquier otro servicio de asistencia domiciliaria a personas vulnerables;
- Reparto de material de protección;
- Facilitar la actuación de voluntariado social en la situación de emergencia.

7. ¿Pueden tener estas actividades de tratamiento cruce de datos entre los distintos departamentos de la entidad local?

Si estos son precisos y se requieren para poder prestar un servicio a la ciudadanía, sí, pero teniendo en cuenta la necesidad y la temporalidad del tratamiento o cruce de datos. Por ejemplo, la información puede ser compartida si la finalidad que se persigue con el tratamiento lo requiere, entre la Policía Local, Recursos Humanos, Servicios Sociales y Salud Pública.

Es importante recordar:
▪ la obligación de confidencialidad al personal del Ayuntamiento que trate los datos;
▪ definir condiciones que aseguren la monitorización activa, es decir trazabilidad y supervisión de los tratamientos;
▪ establecer criterios claros de conservación y/o supresión de los datos;
▪ programar adecuadamente las condiciones y duración del bloqueo posterior de los datos personales.

Además, es necesario asegurar en todo momento la seguridad de los datos personales tratados, especialmente en las actuales situaciones de teletrabajo de acuerdo con las normas de cada organización o en su defecto las de practica reconocida en la administración como puede ser las del CCN:
https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4691-ccn-cert-bp-18-recomendaciones-de-seguridad-para-situaciones-de-teletrabajo-y-refuerzo-en-vigilancia-1/file.html

▪ Se recomienda no permitir la descarga de ficheros con datos personales en discos locales.
▪ Alojar los tratamientos en bases de datos corporativas que prevean su trazabilidad y seguridad.
▪ En caso de tener que recurrir, dada la situación actual, a ficheros ofimáticos, transmitirlos encriptados y enviar las claves a sus destinatarios por una vía alternativa a la utilizada para la transmisión del fichero (ej: fichero encriptado por mail y clave por sms al móvil del destinatario); y almacenarlos en los servidores de ficheros corporativos de forma preferente.

En el documento enlazado se pueden encontrar una guía completa de productos de seguridad y comunicaciones, elaborada por el CCN:
https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html

8. ¿Hay que informar a la ciudadanía de las nuevas actividades de tratamiento?

En la medida de lo posible sí. El RGPD indica que ello no será preciso en la medida en que las personas interesadas ya dispongan de la información; la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular, para el tratamiento con fines de interés público, o en la medida en que la obligación pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento.

No obstante, en estos casos, la entidad local debe adoptar medidas adecuadas para proteger los derechos, libertades e intereses de las personas interesadas, inclusive haciendo pública la información, por ejemplo, por medios electrónicos en el sitio web municipal.

También podría quedar limitada la obligación de informar si la obtención o la comunicación está expresamente establecida por el Derecho de la Unión Europea o nuestro Derecho Interno si establece medidas adecuadas para proteger los intereses legítimos de las personas interesadas.

9. ¿Es posible llevar a cabo una actividad de videovigilancia, ya sea vía drones o mediante cámaras instaladas por la población urbana para identificar conductas prohibidas por la situación de alarma?

Sí, siempre y cuando se tenga en cuenta que esta es una actividad de tratamiento propia de la Policía Local exclusivamente y que está sujeta a los mismos principios del RGPD y la LOPDGDD, como cualquier actividad de vigilancia que ya esté llevando a cabo la Policía Local regulada por la normativa específica de seguridad pública, dado que pese a la característica del medio tecnológico de recogida datos (vehículo aéreo que puede pertenecer a distintas categorías y con diversos sistemas de procesamiento de los datos) al fin y al cabo el dron realiza funciones de captación de imágenes para fines de vigilancia por motivos del COVID-19.

En todo caso, la utilización de drones con el objetivo de implantar una vigilancia general de una población debería tener en cuenta que:

▪ Debe aplicarse la legislación específica:

- La Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
- El Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

▪ Estas videocámaras requieren de un informe favorable de la Comisión de Garantías de la Videovigilancia y de su autorización por el Delegado del Gobierno en la Comunidad Autónoma.
▪ El dron incorpora una videocámara móvil. Conforme al artículo 6.4 de la LO 4/1997 se exige la presencia de un peligro concreto para habilitar el uso de este tipo de cámara.
▪ Deberían evaluarse las condiciones de vuelo del dron de acuerdo con la regulación vigente así como la prohibición expresa de obtener imágenes del interior de las viviendas y de sus vestíbulos. Esta previsión del artículo 6 de la LO 4/1997 debe entenderse que alcanza a patios interiores y zonas reservadas a la vida privada y familiar. El Tribunal Constitucional en su STC 22/1984 considera que una intromisión de esta naturaleza afecta a la inviolabilidad del domicilio y requiere de autorización judicial.
▪ La LO 4/1997 veda expresamente la grabación de conversaciones salvo autorización judicial.

10. **¿Cómo puede informar la entidad local del tratamiento de datos llevado a cabo por drones?**

La normativa no establece una excepción para el tratamiento de datos llevados a cabo por la operativa de drones, por lo que este derecho de información a las personas interesadas habrá de ser cumplido.

Una buena recomendación sería la comunicación "multicanal" habida cuenta de las limitaciones que una aproximación tradicional a la información tiene, por ejemplo, publicándola en la página web municipal, insertando anuncios en periódicos locales, mediante buzoneo, u otras formas.

El anexo del Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, define de modo preciso la señalética y el contenido de la información.

11. ¿Se puede incorporar a las bases de datos municipales información (como teléfonos, datos de contacto u otros) procedente de otras fuentes, como por ejemplo sitios web públicos de internet (guías telefónicas u otros sitios)?

Sí. En estos casos, además de que la base jurídica de tratamiento sea legítima, es muy importante informar a la persona interesada de la fuente de la que proceden los datos personales y de cuáles son los datos personales objeto de tratamiento. Esto puede hacerse de acuerdo con las propuestas antedichas en preguntas anteriores.

Además, esta información se debería hacer constar en el registro de actividades de tratamiento de la corporación local igualmente.

Estas situaciones pueden darse para llevar a cabo actividades especialmente relevantes como, por ejemplo, localizar personas vulnerables (especialmente a través de sus teléfonos) cuyos datos de contacto en algún caso no están en las "fuentes administrativas" del Ayuntamiento o no están actualizados, para lo cual hay que hacer cruces con otros servicios de carácter autonómico como los de salud o con operadores privados de telecomunicaciones o incluso, acudiendo a fuentes públicas en internet.

En todo caso, en todo momento, deberá optarse por la que represente un menor riesgo para los interesados y con fuentes de finalidades compatibles. En este sentido, la Ley de Servicios Sociales prevé la colaboración entre los servicios sociales municipales y los Centros de Atención Primaria (CAPs) para un tratamiento integral de los pacientes y la actuación con medidas coordinadas, ante problemas de salud pública como el actual, permitiendo el intercambio de datos, especialmente los identificativos o de contacto, presentes en los Registros Centrales de asegurados de los servicios sanitarios de las Comunidades autónomas.

En este sentido y atendiendo al principio de minimización de datos y menor riesgo para los derechos y libertades de la persona interesada, es preferible llevar a cabo el intercambio de datos entre las Administraciones públicas antes que el intercambio con otros operadores de índole privada, dado que, en este segundo caso, desde la Administración se podría estar revelando de forma indirecta a estos operadores privados la condición de persona vulnerable, a la hora de solicitar su teléfono (por ejemplo).

12. ¿Puede la entidad local comunicar datos del padrón a otras administraciones públicas?

Sí en la medida en que ello sea necesario dado que el artículo 16.3 de la Ley de Bases de Régimen Local incluye la previsión en relación con la posible cesión de los datos personales de la siguiente forma: "Los datos del Padrón Municipal se cederán a otras administraciones públicas que lo soliciten sin consentimiento previo al afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública y en las leyes de estadística de las comunidades autónomas con competencia en la materia".

13. ¿Es posible comunicar los datos personales a entidades privadas (como ONG, voluntarios, u otros actores similares) para coordinar servicios privados de voluntariado que realizan las mismas funciones que los servicios públicos pero desde asociaciones privadas?

Sí, pero en estos casos conviene adoptar una medida adicional como es la suscripción de un contrato de encargo de tratamiento al amparo del artículo 28 del RGPD, de manera que, finalizada la situación de emergencia que requiere la colaboración con la entidad privada, los datos sean devueltos al Ayuntamiento, destruyendo cualquier copia por parte de la entidad privada.

La necesidad de dar acceso a los datos personales contenidos en las bases de datos del Ayuntamiento a entidades privadas (como listas con nombre de personas de contacto y direcciones) puede surgir del encargo por parte de los Ayuntamientos de servicios como reparto de comidas, reparto de mascarillas, visitas para atender las necesidades de mayores y personas en situación vulnerable u otros fines que deberán ser claramente detallados en el contrato de encargo.

En la medida de lo posible, en todo caso, la contratación de estos terceros debería llevarse a cabo por los cauces habituales de contratación pública local o de emergencia pero siempre incluyendo el contrato de encargo de tratamiento.

(Anexo en página 35)

14. ¿Y en el caso de que estos voluntarios o actores que ayuden a la coordinación de servicios no tengan personalidad jurídica o actúen en su condición de persona física, se les puede igualmente comunicar datos personales?

En estos casos quizás a la entidad local se le complique la posibilidad de llevar a cabo la firma de un contrato de encargo de tratamiento, fundamentalmente en caso de que la ayuda para la realización de las tareas sea llevada a cabo por un grupo de personas voluntarias que no se han constituido como agrupación bajo ninguna forma jurídica.

Como medida mínima a ejecutar por el Ayuntamiento en estos casos es imprescindible trasladar a la/s persona/s que vayan a prestar el servicio o colaboración las instrucciones precisas para que el Ayuntamiento no pierda el control sobre los datos que son puestos a su disposición así como concienciar a dichas personas que solo deben usarlos de forma estrictamente confidencial y siembre bajo las instrucciones de tratamiento del Ayuntamiento.

Por tanto, el Ayuntamiento debe trasladar a las personas físicas las instrucciones del encargo de tratamiento de los datos, en la medida de lo posible acercándose en su redacción a lo establecido en el artículo 28 del RGPD.

A estos efectos se aporta como **ANEXO I** a este documento un modelo de instrucciones de encargo de tratamiento.

15. ¿Puede la entidad local realizar un mapa epidemiológico indicando las zonas de desarrollo de COVID-19 en la población y su porcentaje?

Sí. El derecho a la protección de datos no es incompatible con el monitoreo epidemiológico, enfatizando que los datos anonimizados no están cubiertos por los requisitos de protección de datos. Por lo tanto, el uso de información agregada para señalar zonas de alta, media o baja incidencia de la enfermedad en el territorio municipal no vulnera la normativa de protección de datos.

No obstante, el Ayuntamiento deberá tener en cuenta que cuanto mayor sea el grado de información estadística más deben tenerse en cuenta medidas que aseguren la anonimización. En la publicación de información estadística que incluya datos relativos a edad, género, indicadores sociales etc., deberá tenerse muy en cuenta el impacto del tamaño poblacional del área en la identificabilidad de las personas.

16. ¿Y se puede tratar el dato de la geolocalización de las personas?

En primer lugar, entenderemos por geolocalización la ubicación en coordenadas absolutas de un terminal, bien sea mediante el seguimiento de los sistemas GPS integrados o del posicionamiento celular que pueden realizar las compañías operadoras.

No debe confundirse con los sistemas de localización próxima que como el Bluetooth que permitiría establecer relaciones de proximidad entre dispositivos, pero no conocer su localización en términos de posición absoluta.

La Orden SND/297/2020 de 27 de marzo, regula en su punto segundo encomendar a la Secretaría de Estado de Digitalización y Inteligencia Artificial el estudio de la movilidad de las personas en los días previos y durante el confinamiento siguiendo el modelo agregado y anonimizado ya utilizado previamente por el INE con los datos provenientes de las operadoras del servicio.

Asimismo, en el punto tercero, encomienda a dicha Secretaría ser el punto central de la coordinación para la evaluación de otras propuestas tecnológicas por parte de otros organismos y entidades, entre los que deberemos incluir también las posibles propuestas de las EELL.

Por lo que cualquier posible tratamiento al respecto, deberá hacerse dentro de este marco, de forma agregada, con las debidas garantías de irreversibilidad del proceso y de acuerdo con la citada Orden.

17. ¿Puede la entidad local tratar los datos del padrón para que la Policía Local o los bomberos feliciten el cumpleaños de las personas censadas en su municipio en el marco de la adopción de medidas para generar el bienestar y distensión de la población?

El uso del padrón municipal para los fines indicados puede entenderse dentro del ejercicio de las competencias municipales siempre que se lleve a cabo en el marco de la función de integración social de la población, cultivar los lazos de unión, evitar el desarraigo o generar el bienestar y distensión de la población pero, no se debe utilizar previa elaboración de perfiles y haciendo públicos los datos personales, sin que en este último caso previamente se obtenga el consentimiento de las personas interesadas.

Si el Ayuntamiento desea llevar a cabo alguna comunicación o felicitación personalizada de forma pública, será preciso que obtenga previamente el consentimiento de la persona interesada, especialmente en el caso de tratamiento de menores, lo cual puede llevar a cabo a través de diversas formas:

- Informando a la ciudadanía de la posibilidad de llevar a cabo este tipo de iniciativas a efectos de lo cual, las personas interesadas pueden solicitar su participación a través de la cumplimentación de un formulario web autorizando el tratamiento de sus datos personales o el de menores bajo su representación o tutela legal.
- Habilitando para la ciudadanía un canal telefónico donde llevar a cabo la misma solicitud.

Es preciso advertir que el padrón municipal no habilita *per se* este uso de los datos personales para felicitar públicamente a la ciudadanía de forma personalizada, por lo que si bien desde el Ayuntamiento es posible identificar la fecha de nacimiento de los vecinos, debe llegar **¿?** las familias y personas titulares de los datos (incluso en colaboración con las entidades del barrio o las escuelas) para, de forma previa a tratar los datos para estas iniciativas, obtener la autorización de las personas interesadas.

En todo caso, cualquier acción municipal llevada a cabo en esta línea, debe garantizar la protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen y llevarse a cabo dentro de los usos sociales.

18. ¿Puede la entidad local llevar a cabo tratamientos incluyendo datos personales en redes sociales o sitios web municipales para fines como la redacción de un diario digital con vídeos, imágenes u otros datos que incluyan información sobre menores, mayores o de personas en situación de riesgo o vulnerables para generar el bienestar y distensión de la población?

Sí, siempre que se realice mediante un consentimiento explícito que podría obtenerse a través de la cumplimentación previa de un formulario web.

En el caso en que en las redes sociales oficiales sean terceras personas (por ej. vecinos o vecinas) quienes publiquen los datos en estas redes municipales, se les exigirá a través de una política o código de comportamiento, el cumplimiento de unas reglas que garanticen el cumplimiento de la normativa de protección de datos y derecho a la intimidad y propia imagen, como, por ejemplo, las siguientes:

▪ No publicar imágenes de personas sin su permiso o autorización.
▪ Evitar las imágenes que puedan identificar a menores pese a ser su padre, madre o tutor legal.
▪ Las reglas habituales de ética y estética para no invadir el derecho al honor, intimidad personal y familiar.

Será el Ayuntamiento quien, en todo caso, deberá llevar a cabo la redacción de estas “reglas” y su publicación en los canales municipales oficiales de comunicación (incluidas las redes sociales) a través de un comité creado al efecto que también se encargará de verificar el cumplimiento de estas reglas.

No obstante, lo anterior debe entenderse sin perjuicio de los supuestos del ejercicio del derecho a la información amparados constitucionalmente que pueda llevar a cabo el Ayuntamiento a través de sus canales de comunicación.

19. ¿Puede la entidad local poner a disposición de la ciudadanía herramientas para el envío de mensajes, imágenes u otros contenidos para expresar los sentimientos de la ciudadanía y llevar a cabo su difusión pública?

Sí. Pero habría que tener en cuenta que si de lo que se trata es de habilitar una plataforma donde se puedan dejar mensajes, será importante valorar específicamente los siguientes aspectos:

El primero, el de la titularidad de la plataforma. Si la plataforma donde se almacenarán los datos y desde donde se difundirán a la ciudadanía no es propiedad de la entidad local, será preciso que el Ayuntamiento, cuando contrate el uso de la plataforma, suscriba un contrato de encargo de tratamiento con su titular. Esto es complicado cuando las plataformas que se utilizan para ello son plataformas sociales comerciales del tipo whatsapp. Por ello, lo idóneo sería que la plataforma fuera local o de un proveedor con quien el Ayuntamiento tuviera capacidad de negociación para establecer las condiciones del encargo de tratamiento. Véase en Barcelona recorda un ejemplo de este servicio.

El segundo, la necesidad de que para hacer uso del servicio existan unas normas de uso o condiciones de participación en el servicio por parte de la ciudadanía, en las cuales quede explicado el alcance del mismo así como las condiciones de tratamiento de los datos (incluyendo las condiciones del artículo 13 y 14 del RGPD o remisión al correspondiente registro de actividad), derechos de imagen (explicando las garantías previstas de acuerdo con el derecho al honor intimidad personal y familiar), derechos de propiedad intelectual (para no incurrir además en infracciones de esta normativa) y moderación del servicio. En estas condiciones se pueden incluir las “normas de estilo” de los mensajes que los ciudadanos quieran difundir. Véase un ejemplo de condiciones de participación.

El tercero, sería conveniente la creación de un Comité que supervise que todos los mensajes y publicaciones que se emiten cumplen los criterios o normas de estilo y términos de las condiciones de uso.

Es preciso recordar que si la plataforma utilizada por el Ayuntamiento para un servicio de este estilo es una plataforma o red social comercial, las anteriores condiciones deberán ser previstas igualmente por el Ayuntamiento, con la dificultad que ello conlleva; asimismo, la ciudadanía deberá cumplir, además de las condiciones de la entidad local, las establecidas por el titular de la plataforma social.

20. ¿Puede la entidad local poner a disposición de la ciudadanía un teléfono de mensajería instantánea para informar sobre actuaciones y medidas con relación al COVID-19?

Sí, para proporcionar información general de interés, así como información de los servicios del Ayuntamiento.

Únicamente habría que tener en cuenta que, en el caso de que a través de estos servicios la ciudadanía proporcionase datos personales (véase por ej. dar su dirección para recibir un servicio) sería conveniente adaptar la información a proporcionar a las personas interesadas, en virtud de los artículos 13 y 14 del RGPD a través de locuciones telefónicas con remisión al registro de actividades o política de privacidad en la web municipal.

21. ¿Puede la entidad local crear aplicaciones móviles o webs temáticas destinadas a la autoevaluación del coronavirus por las personas interesadas?

Las competencias sanitarias están reservadas al Estado y a las Comunidades Autónomas.

Por tanto, el primer paso para poner en práctica estos servicios debe ser verificar que el Ayuntamiento dispone o tiene atribuidas competencias en materia sanitaria que le permitan crear aplicaciones con fines de autoevaluación previa recogida de datos personales puesto que, en general, estas funciones solo están atribuidas a Ayuntamientos de grandes poblaciones.

En caso de que el Ayuntamiento no tenga atribuidas estas competencias (las cuales por su propia naturaleza están restringidas a las autoridades sanitarias) los Ayuntamientos no podrán elaborar herramientas para la gestión de este tipo de funciones.

Por tanto, si el Ayuntamiento puede justificar, en el marco de su ámbito competencial, la existencia de competencias sanitarias, el uso de estos medios no es incompatible con la normativa de protección de datos.

22. ¿Puede una entidad local crear aplicaciones móviles o webs temáticas destinadas a asuntos relacionados con el coronavirus en el marco de las competencias de asuntos sociales u otros?

Sí. Teniendo en cuenta lo indicado en la pregunta anterior (esto es, excluyendo cualquier actividad o función relacionada con las competencias sanitarias que están reservadas a las Comunidades Autónomas) desde áreas como los servicios sociales si pueden crearse herramientas para la gestión propia de las competencias de esa área en concreto.

Además, es posible que las áreas de servicios sociales tengan funciones de ayuda o colaboración con las Administraciones Públicas, de la Comunidad Autónoma o del Estado, con competencias sanitarias.
Por tanto, desde las entidades locales sí es posible llevar a cabo estas funciones de apoyo y colaboración con las Administraciones Públicas con competencias sanitarias mediante habilitación de herramientas específicas al efecto. Pero es importante que en estos casos queden claras las competencias, funciones y responsabilidad de los tratamientos de datos de cada Administración en función de sus competencias a través de convenios u otros instrumentos jurídicos al efecto.

23. ¿Y en caso de que se creen aplicaciones móviles o webs temáticas en el marco de la gestión de las competencias locales, qué debe tener en cuenta el Ayuntamiento respecto de las mismas?

Una vez que el Ayuntamiento decide la creación de aplicaciones móviles o webs temáticas para la gestión de sus competencias en algún área, por ej. en el área de servicios sociales, es importante que tenga en cuenta los siguientes pasos:

▪ Garantizar que el desarrollo y uso de la aplicación se relacione directamente con el ejercicio de competencias de la Administración Local y ello se pueda justificar.
▪ Diseñar o seleccionar la herramienta bajo el principio de privacidad desde el diseño y por defecto.
▪ Vinculado al punto anterior, es preciso extremar el rigor en el cumplimiento del RGPD y en particular en la definición de la finalidad y la proporcionalidad tanto en los permisos de la aplicación como en las categorías de datos personales objeto de tratamiento.
▪ Valorar la necesidad de realizar una evaluación de impacto en la protección de datos para determinar el tipo de medidas que se deben establecer en las herramientas en función de cómo se lleve a cabo el tratamiento de los datos.
▪ El diseño de cómo se garantizará la visibilidad de los textos legales informativos del alcance del tratamiento de datos (incluyendo fines de tratamiento, destinatarios y derechos) así como la forma de obtención de los consentimientos es también muy relevante.
▪ Revisar las guías y recomendaciones a seguir elaboradas por las autoridades de control, todo ello para incorporar las medidas que requiere el RGPD y la LOPDGDD que ya se han mencionado en respuestas anteriores.
▪ Y tener en cuenta que si las herramientas son desarrolladas por un tercero deberá incluirse de modo expreso en el contrato de encargado del tratamiento el deber de usar metodologías de protección de datos desde el diseño y por defecto que permitan a la entidad local cumplir con el RGPD y LOPDGDD. En este sentido se exigirá al tercero que utilice una metodología de desarrollo reconocida tomando en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida y previa aceptación y puesta en servicio se someterá a un análisis de vulnerabilidades y pruebas de penetración.
▪ No olvidar que es fundamental el trabajo del delegado de protección de datos durante el proceso de análisis, desarrollo, programación y test previo a producción de la aplicación.

Con el fin de que la Entidad del Sector Público conozca con precisión dónde se encuentran físicamente alojados sus sistemas de información y su información, el prestador de servicios aportará la documentación que detalle si los tratamientos de información van a ejecutarse en sistemas e instalaciones propias o de la Entidad del Sector Público. Asimismo, en caso de que los tratamientos se realicen en sistemas del prestador del servicio, se indicarán las medidas de seguridad física asociadas.

Hacemos especial hincapié en que exista una completa y transparente política de privacidad accesible por las personas usuarias de la aplicación o de la web, textos informativos claros y

accesibles en los formularios de recogida de datos y todo ello en coherencia con el correspondiente enlace al registro de actividad publicado de forma electrónica por la entidad local.

24. ¿Cuál es el plazo de conservación de los datos de carácter personal recogidos por el Ayuntamiento en el marco de las acciones llevadas a cabo para la prevención y gestión del COVID-19?

En el marco de la prevención y gestión del COVID-19 los Ayuntamientos pueden haber llevado a cabo la recogida y tratamiento de datos personales de diversa naturaleza como hemos ido viendo a lo largo de todo el documento (en especial los que se encuentren en el ámbito del art.9 del RGPD).

Es tarea del Ayuntamiento determinar los plazos de conservación de la información que contenga dichos datos personales o, en su caso, el proceso de bloqueo, pseudoanimización o anonimización completa en función de los criterios que se establezcan por cada servicio municipal y en la legalidad vigente una vez finalizada la situación especial generada por el estado de alarma o cualquier otra norma con rango legal que le pudiera suceder.

En este sentido deberá tenerse en cuenta si, tanto los servicios sociales como en su caso los servicios de salud pública (de acuerdo a las competencias municipales al respecto), deban conservar estos datos personales y mantener determinados tratamientos de datos, cuando pudieran existir algunos escenarios como los que citamos a continuación:

- El impacto social y económico de la enfermedad puede obligar a mantener, con posterioridad al período de alarma sanitaria, la necesidad de políticas públicas de igualdad que puedan requerir identificar a afectados, personas vulnerables o familias especialmente golpeadas.
- Que se produzca la aparición de un segundo brote, donde las víctimas de la primera podrían ser sujetos especialmente vulnerables.
- Analizar, a la luz de la información obtenida, necesidades de mejora o modificación de los servicios municipales para poder atender a la ciudadanía en mejores condiciones, al finalizar la situación de crisis.

Siempre será preciso que el Ayuntamiento, continúe aplicando, en todo momento, los principios del RGPD, especialmente, en lo referido a transparencia, minimización o seguridad y de forma muy especial con su legitimación, dado que por ejemplo el tratamiento de los datos de salud, podrían estar limitados al período del estado de alarma.

Para ello, se sugiere separar los datos sanitarios~~,~~ de otros de tipo social, para los que las EELL ya están legitimadas en sus funciones de servicios sociales, o generar sistemas de agregación, pseudonimización o anonimización que garanticen la irreversibilidad de los datos personales protegidos en el nuevo escenario normativo que, en cualquier caso, siempre será el que marque el final de la conservación legal de los mismos.

25. ¿Son importantes las políticas internas de protección de datos de las entidades locales?.

Sí y mucho. Aunque, a priori, su función es interna y tienen como fin garantizar la gobernanza de la protección de datos dentro de la entidad local de acuerdo con los principios y garantías del RGPD y la LOPDGDD, la crisis ha desatado rumores, acusaciones, pronunciamientos alarmistas que disuaden a la sociedad de confiar el tratamiento de los datos. Por ello, las políticas y la transparencia de los tratamientos de datos informando a las personas interesadas y publicando los registros de actividades que sean objeto de nueva creación, contribuyen a ofrecer seguridad y tranquilidad a la ciudadanía.

26. ¿Es posible la utilización de sistemas de videollamadas para la realización de Plenos y Juntas de Gobierno?

La evolución de la pandemia marcada por Covid-19 ha traído consigo el uso generalizado de videoconferencias. En este sentido, El Real Decreto-ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente al COVID-19 (Ref. BOE-A-2020-4208) modifica el artículo 46 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, añadiendo un nuevo apartado 3, en virtud de la disposición final 2 del citado Real Decreto-ley:

> *"En todo caso, cuando concurran situaciones excepcionales de fuerza mayor, de grave riesgo colectivo, o catástrofes públicas que impidan o dificulten de manera desproporcionada el normal funcionamiento del régimen presencial de las sesiones de los órganos colegiados de las Entidades Locales, estos podrán, apreciada la concurrencia de la situación descrita por el Alcalde o Presidente o quien válidamente les sustituya al efecto de la convocatoria de acuerdo con la normativa vigente, constituirse,* ***celebrar sesiones y adoptar acuerdos a distancia por medios electrónicos y telemáticos, siempre que sus miembros participantes se encuentren en territorio español y quede acreditada su identidad****. Asimismo, se deberá asegurar la comunicación entre ellos en tiempo real durante la sesión, disponiéndose los medios necesarios para garantizar el carácter público o secreto de las mismas según proceda legalmente en cada caso.*
>
> *A los efectos anteriores,* ***se consideran medios electrónicos válidos las audioconferencias, videoconferencias, u otros sistemas tecnológicos o audiovisuales que garanticen adecuadamente la seguridad tecnológica****, la efectiva participación política de sus miembros, la validez del debate y votación de los acuerdos que se adopten".*

A estos efectos, debe tenerse en cuenta que las aplicaciones de videoconferencia que no estén adecuadamente protegidas pueden suponer un vector de ataque.

Esta modificación se contempla específicamente para los órganos de gobierno de la Administración local y en una serie de supuestos excepcionales. En el caso del Pleno, el artículo 70. 1 de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local, preceptúa expresamente el carácter público de las sesiones de los plenos, por lo que, con carácter general, dichas sesiones serán objeto de publicación, bien en streaming o en diferido.[1]

Como premisa de partida, una adecuada implementación de la solución respetando unos mínimos requisitos de seguridad en la configuración y la creación de unas normas de uso, harán factible la puesta en marcha de este tipo de soluciones.

En este sentido, el Centro Criptológico Nacional ha publicado un documento de ciberconsejos en el uso de sistemas de videollamadas~~.~~, donde se indican las diferentes recomendaciones de seguridad (convocatorias, limitación de acceso a terceras personas, etc.)

1 No obstante, podrán ser secretos el debate y votación de aquellos asuntos que puedan afectar al ~~3~~ derecho fundamental de los ciudadanos a que se refiere el artículo 18.1 de la Constitución, cuando así se acuerde por mayoría absoluta

27. **¿Qué aspectos debemos tener en cuenta para poner el teletrabajo?**

A raíz de la pandemia, las entidades locales han adaptado su forma trabajar para hacer frente a estos momentos complicados, en los que se incluye, entre otras, el teletrabajo, aspecto que genera grandes oportunidades. Estas oportunidades, lamentablemente, también amplían las posibilidades de los ciberdelincuentes, que encuentran nuevas vías de atacar a nuestras organizaciones, poniendo en riesgo los datos personales.

La suma de una puesta en producción acelerada, a nivel masivo de accesos remotos, unida a la falta de costumbre en este tipo de accesos para algunas personas, eleva considerablemente el riesgo a sufrir incidentes de seguridad de diferente índole.
En este sentido, el Centro Criptológico Nacional ha publicado un Informe de Buenas Prácticas bajo el título de: CCN-CERT BP/18 Recomendaciones de Seguridad para situaciones de teletrabajo y refuerzo en vigilancia, así como un documento sobre Acceso Remoto Seguro, donde se proporcionan una serie de soluciones que permiten implementar, de forma ágil, acceso remoto a los recursos de una Organización minimizando el impacto en los recursos IT y optimizando el tiempo para su puesta en producción.

Con independencia de la solución técnica seleccionada, es muy importante documentar las decisiones tomadas por el comité de crisis en la activación del teletrabajo, documentando los riesgos inherentes a su puesta en marcha, así como las principales medidas implementadas para minimizarlos.

28. ¿Cómo incide esta situación sobre nuestro deber de diligencia debida exigido por el RGPD en los procesos de contratación pública?

A pesar de que el derecho a la protección es un derecho fundamental, debemos mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.

No obstante, las entidades del Sector Privado cuando provean de servicios o soluciones, sujetos al cumplimiento del Esquema Nacional de Seguridad, a las Entidades Públicas, deberán estar en condiciones de exhibir, respecto a estos, la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA, de acuerdo a lo establecido en la "Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad", aprobada el 13 de octubre de 2016, por Resolución de la Secretaría de Estado de Administraciones Públicas.

Es responsabilidad de las entidades públicas contratantes notificar a los operadores del sector privado que participen en la provisión de soluciones tecnológicas o en la prestación de servicios, la obligación de que tales soluciones o servicios sean conformes con lo dispuesto en el Esquema Nacional de Seguridad y posean las correspondientes Declaraciones o Certificaciones de Conformidad, según lo señalado en la mencionada Instrucción Técnica de Seguridad.

Para soluciones "on premise", será de aplicación también lo indicado en el "Abstract-Requisitos de Seguridad Adicionales para Servicios en la Nube prestados desde instalaciones en modo local", en particular en lo relativo a los requisitos de seguridad adicionales (Guía de Instalación y Configuración Segura del Sistema destinada a administradores y la Guía de Uso Seguro del Sistema destinada a usuarios finales).

Anexo a pregunta 13.

¿Y en el caso en que estos voluntarios o actores que ayuden a la coordinación de servicios no tengan personalidad jurídica o actúen en su condición de persona física, se les puede igualmente comunicar datos personales?

INSTRUCCIONES DE ENCARGO DE TRATAMIENTO

Los abajo firmantes (en adelante denominados conjuntamente ENCARGADO DEL TRATAMIENTO) personas voluntarias vinculadas al servicio _____ del Ayuntamiento de _____ **DECLARAN,**

I.- Que de forma voluntaria participan en la prestación de servicios de _____ al Ayuntamiento.

II.- Que en el marco de los servicios que se prestarán, los datos personales solo podrán ser tratados con los siguientes fines:
_____
_____
_____

III.- Que en el desarrollo de las actividades a realizar en el marco de los servicios indicados en el apartado anterior, el Ayuntamiento pondrá a disposición del ENCARGADO DEL TRATAMIENTO datos personales de las siguientes categorías de personas:
_____
_____
_____

IV.- Que respecto de las categorías de personas indicadas en el apartado anterior, el Ayuntamiento permitirá el acceso a los siguientes datos personales:
_____
_____
_____

Visto lo anterior, el ENCARGADO DEL TRATAMIENTO tratará los datos personales con los fines indicados en los apartados anteriores, de acuerdo con las siguientes, **INSTRUCCIONES DE TRATAMIENTO DE DATOS**

El ENCARGADO DEL TRATAMIENTO se compromete a:

a) tratar los datos personales únicamente de acuerdo con las presentes instrucciones.
b) respetar la confidencialidad y el deber de sigilo de los datos personales, obligaciones que subsistirán aun después de finalizar sus relaciones con el citado proyecto;
c) no ceder datos ni alojarlos en servicios provistos por un tercero.
d) devolver todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimiendo las copias existentes a menos que se requiera la conservación de los datos personales en virtud de una obligación legal;
e) poner a disposición del Ayuntamiento toda la información necesaria para demostrar el cumplimiento de estas obligaciones y contribuir a la realización de auditorías, incluidas inspecciones, por parte del Ayuntamiento o de otro auditor autorizado por la citada entidad;
f) no utilizar, en ningún caso, los datos para fines propios y, particularmente, para la prestación de servicios profesionales a las personas interesadas.;
g) asistir al Ayuntamiento en la atención de los derechos de protección de datos de las personas interesadas;
h) notificar al Ayuntamiento la existencia de brechas o violaciones de seguridad;
i) nombrar un interlocutor que estará en contacto con el Ayuntamiento para el correcto control y ejecución de las instrucciones contenidas en el presente documento;
j) custodiar los datos de forma segura, dando cumplimiento a las siguientes **MEDIDAS DE SEGURIDAD:**

Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el

responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular, como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Información sobre el tratamiento de datos de carácter personal: todas las partes firmantes del presente documento quedan informadas del tratamiento de sus datos de carácter personal, de acuerdo con lo siguiente:

Responsable del tratamiento: Ayuntamiento de _____ con dirección postal _____ y electrónica _____.

Datos de contacto del delegado de protección de datos del Ayuntamiento: _____

Base jurídica y fines del tratamiento: con base jurídica en el cumplimiento de obligaciones legales y para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, los datos serán tratados para llevar a cabo la firma, ejecución, justificación y control del cumplimiento del presente contrato.

Necesidad del tratamiento; la comunicación de datos personales a los efectos expuestos en el apartado anterior es un requisito necesario para la suscripción del presente contrato y la persona interesada está obligada a facilitar los datos personales quedando informada de que en caso de no facilitar tales datos serán de aplicación las consecuencias previstas en el Ordenamiento Jurídico.

Destinatarios: En cumplimiento de las obligaciones legales, los datos personales serán comunicados a las autoridades y administraciones públicas competentes por razón de la materia. Asimismo, podrán ser puestos a disposición de terceros para el tratamiento de datos por encargado del Ayuntamiento.

Transferencias internacionales de datos: Los datos personales no serán objeto de transferencias internacionales.

Derechos: Las personas interesadas tienen derecho a solicitar el acceso a sus datos personales, la rectificación, supresión, oposición, limitación del tratamiento, no ser objeto de una decisión basada únicamente en el tratamiento automatizado de los datos, incluida la elaboración de perfiles, dirigiéndose al Ayuntamiento a través de cualquiera de las siguientes direcciones:
Postal:_____
Electrónica: _____
El ejercicio de los derechos es personalísimo y requerirá la identificación inequívoca de la persona interesada, que podrá realizarse mediante la aportación de su documento nacional de identidad, pasaporte u otro documento válido que la identifique así como instrumentos electrónicos equivalentes.

Derecho a reclamar: La persona interesada puede presentar una reclamación ante la Agencia Española de Protección de Datos a través de la sede electrónica accesible a través de la página web https://www.aepd.es/. Con carácter previo, las personas interesadas pueden contactar con el delegado de protección de datos del Ayuntamiento a través de _____

Y, a tal efecto en _____ a ____ de _____ 20___ lo suscriben en nombre y por cuenta de ENCARGADO DEL TRATAMIENTO los siguientes participantes:

Nombre y apellidos	DNI a	Firma

Nombre y apellidos	DNI a	Firma

Nombre y apellidos	DNI a	Firma