Islas Canarias
Del 15 al 19 de noviembre de 2021

El Registro de Actividades de Tratamiento a partir del RGPD, 2018

Usua Galarza Martinez de Ubago
Referente de Seguridad
u-galarza@eustat.eus

Jesús Nieto Gonzalez
Referente de Seguridad
j-nietogonzalez@eustat.eus

1. Introducción a la protección de datos personales.

- Ordenamiento jurídico (fuentes de derecho).

2.1.Reglamento europeo (RGPD)

- Incorporación de nuevos **roles**.
  - Responsable de tratamiento (controller): Director
  - Encargado del tratamiento (processor): hacedor de la operación
  - Delegada de protección de datos DPD (officer): A nivel de Gobierno Vasco.
  - Responsable de medidas de privacidad: Subdirectora del Área de Coordinación Técnica
  - Referente de seguridad: 2 personas, una con perfil técnico informático y otra con perfil legal.
- Establecimiento de una **responsabilidad proactiva**: responsable de cumplir y capaz de demostrar.
  - Somos responsables de cumplir y debemos ser capaces de demostrar que cumplimos.
  - Elementos/Herramientas que forman la responsabilidad proactiva:
    - Registro de actividades de tratamiento.

        - Privacidad desde el diseño y por defecto (seudonimización, minimización de datos, cifrado, …).
        - Seguridad basada en gestión de riesgos.
        - Evaluación del impacto sobre la privacidad.
        - Códigos de conducta y certificaciones.

- Fijación de nuevos **principios** relativos al tratamiento de datos.
    - Respecto al interesado:
        - Lealtad
    - Respecto al tratamiento:
        - Transparencia.
        - Licitud (o legitimación).
        - Limitación de la finalidad.
    - Respecto a los datos:
        - Pertinencia y Minimización.
        - Exactitud y vigencia.
        - Limitación del plazo de conservación.
        - Integridad y confidencialidad.

2.2. Ley Orgánica estatal – LOPDyGDD.

- **Registro de las actividades de tratamiento**. Artículo 31
    - Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento.
    - El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo
    - Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.
- **Transparencia y deber de información**.
    - Disposición adicional 2ª y final 11ª. Modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
        - Publicación del inventario de tratamiento de datos.

- El RAT es la base de la transparencia, pero el RGPD añade requisitos adicionales en cuanto a la necesidad de informar a las personas interesadas, generalizando el concepto de "Tratamiento".

- Para hacer compatible la mayor exigencia de información y deber de transparencia que introduce el RGPD y la concisión y comprensión en la forma de presentarla, desde las Autoridades de Protección de Datos se recomienda adoptar un modelo de información por capas o niveles (más adelante).

- **Carácter obligatorio en el ámbito estadístico**: Art 25.2 Tratamiento de datos en el ámbito de la función estadística pública.

  - Excepción. Art 11.2 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, los datos serán de aportación estrictamente voluntaria.

2. Medidas a adoptar.

3.1. Pasos para la implementación.

- Guía de 8 pasos (Publicación conjunta de las agencias de protección de datos)

  1. Designar un Delegado de Protección de Datos (DPD).
  2. **Establecer el Registro de Actividades de Tratamiento.**
  3. Revisar la legitimación de los tratamientos.
  4. Revisar la información que se ofrece a los interesados.
  5. Revisar los procedimientos de ejercicio de derechos.
  6. Revisar los contratos con Encargados de Tratamiento.
  7. Efectuar Análisis de Riesgos y revisar las medidas de seguridad.
  8. Determinar la necesidad de efectuar Evaluaciones de Impacto.

- Guías, herramientas y normativas.

  - Guía del reglamento general de protección de datos para responsables de tratamiento. General

  - Adecuación de las administraciones públicas al Reglamento General de Protección de Datos: Guía en 8 pasos. Proceso de implementación que estamos tratando.

  - Guía para el cumplimiento del deber de informar. Punto 4 de la implementación, que exponemos en el siguiente punto 2.2.

  - Directrices para la elaboración de contratos entre responsables y encargados del tratamiento. Punto 6 de la implementación.

  - Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. Punto 7 y 8 de la implementación.

- Guía de Protección de Datos por Defecto. Objetivo de implementación con calidad.

- Medidas organizativas.
  - Designación de los roles de seguridad en protección de datos.
  - Registro de activos implicados en los tratamientos. Embrión del RAT.
  - Implantación de políticas de privacidad y protección de datos.
  - Formación del personal en materia de protección de datos de carácter personal.
  - Protocolo de Seguimiento:
    - Establecimiento de un registro de incidencias.
    - Comunicación con Delegada de Protección de Datos (Brechas de seguridad, Estandarización, …).
  - Realización periódica de auditorías.

3.2. El deber de informar.

Guía para el cumplimiento del deber de informar (Publicación conjunta de las agencias de protección de datos)

- RAT y deber de transparencia e información a los interesados
- Cambios el RGPD sobre el deber de informar:
  - **Quién**: El responsable del tratamiento
  - **Cuándo**:
    - Si los datos se obtienen directamente del interesado.
    - Cuando no se obtienen del propio interesado.
  - **Dónde**: Entrevista telefónica, formularios de papel, navegación o formularios Web, …
  - **Cómo**: De fácil acceso, inteligible, lenguaje claro, sencillo, de forma concisa y transparente.
- **QUÉ** se informa/Información por capas:

  Para cumplir con la exigencia que establece el RGPD de mayor información desde las Autoridades de Protección de Datos se recomienda implantar un modelo de información por capas o niveles.
  - presentar una información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos

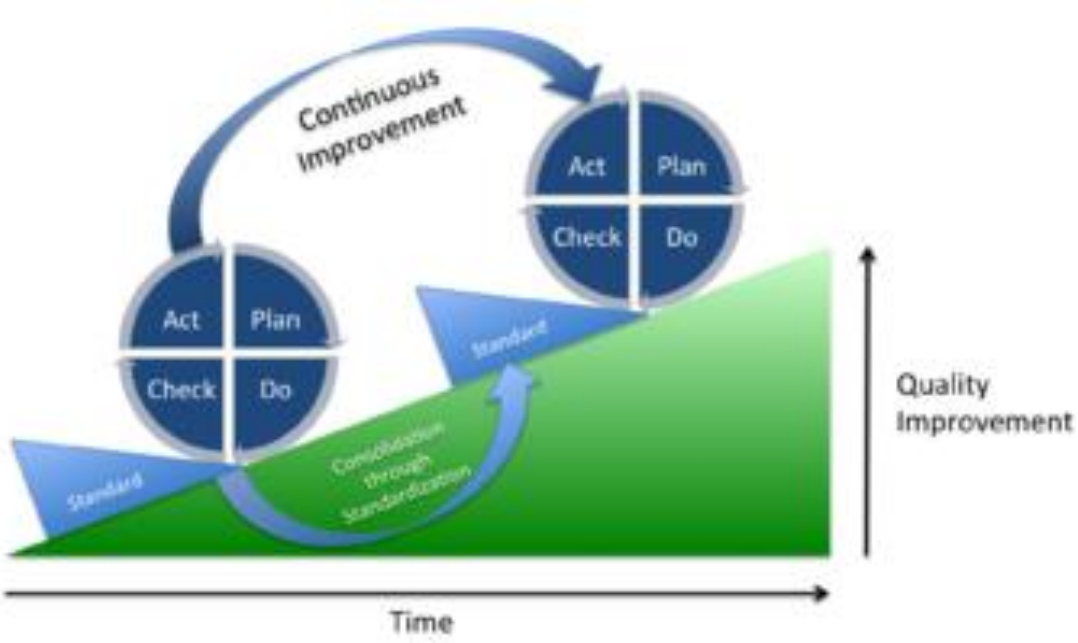
- remitir a la información adicional en un segundo nivel, donde se presentarán detalladamente el resto de las informaciones, en un medio más adecuado para su presentación, comprensión y, si se desea, archivo.
- Información básica (primera capa).
- Información adicional (segunda capa).

- Ejemplos del deber de informar: encuesta, llamada telefónica, …

3.3. Ejercicio de derechos.

- Art 12 LOPDYDGG. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado
- **Derechos**:
  - Derecho de acceso al interesado.
  - Derecho de rectificación.
  - Derecho de supresión.
  - Derecho a la limitación del tratamiento.
  - Obligación de notificación relativa a la rectificación o supresión o la limitación del tratamiento.
  - Derecho a la portabilidad de los datos.
  - Derecho de oposición.
  - Decisiones individuales automatizadas, incluida la elaboración de perfiles.
- Menores de 14 años.
- Gratuidad.
- Excepción de derechos LOPDYGDD. Tratamiento de datos en el ámbito de la función estadística pública.

3. Implementación del RAT.



3.1. Ciclo PDCA.

- PDCA (Plan, Do, Check, Act)
  - **Primer ciclo PDCA, planificación**:
    - Punto de partida: declaración de ficheros en AVPD.
    - RAT versión 0: reconvertir las declaraciones de ficheros y agruparlos en tratamientos de datos.
    - RAT versión 1: colaborativa entre todo el instituto.
    - Siguientes ciclos, se elaborarán siguiendo el principio de "Protección de datos por defecto y desde el diseño": modificación automatizada en función del propio procedimiento de puesta en marcha de las operaciones estadísticas (o de la modificación o creación de actividades administrativas).
  - Primer ciclo PDCA, ejecución:
    - Listamos los ficheros de datos declarados en la AVPD (Agencia Vasca de Protección de Datos).
    - Agrupamos los ficheros por "actividades de tratamiento generales", en aras de poder mostrar un RAT simple y comprensible para el ciudadano.
    - Incluimos la actividad de tratamiento "Producción estadística", que previamente no estaba declarada como fichero, al no ser exigido por la LOPD 15/1999.
  - **Obtención del RAT versión 0 (RATv0).**
  - Primer ciclo PDCA, verificación y corrección:

- Verificamos que las nuevas actividades tengan las mismas bases jurídicas y legislación aplicable.
- Creamos un modelo para la recogida estructurada de los datos personales que se tratan en cada actividad, que debe ser rellenada por su responsable.
    - Nos damos cuenta que hemos agrupado demasiado la actividad de "Producción estadística" y deberemos desagruparla en una siguiente fase.
- Verificamos que las actividades declaradas pueden contener todas las aplicaciones informáticas y actividades tratamiento de datos personales realizadas por Eustat.
- Verificamos que el RAT propone una información comprensible de lo que hace Eustat para el ciudadano.
- Se propone a la Delegada de Protección de Datos para su publicación en el RAT de Gobierno Vasco. Se producen:
    - Ajustes de estandarización (con el resto de actividades declaradas en Gobierno), modelizando actividades comunes (gestión de contactos, recursos humanos, …)
    - Corrección de errores.

- **Obtención del RAT versión 1 (RATv1).**
- Segundo ciclo PDCA, planificación y ejecución:
    - Según planificado en PDCA ciclo 1, desdoblamos la actividad de producción estadística, eliminándola y creando en su lugar tantas actividades como operaciones estadísticas con tratamientos de datos personales haya.
        - Se pasa el modelo de recogida de datos personales tratados.
    - Incorporamos las correcciones / cambios detectados, desde la implantación RATv1, al registro de tratamiento:
        - Nueva actividad, no declarada anteriormente, de Depósito y gestión de copias de padrones municipales.
        - Desdoblamiento de la actividad de Difusión y gestión de peticiones en dos (aislar existencia de consentimiento en la difusión).
        - Modificaciones menores de colectivos, categorías de datos, …
- Segundo ciclo PDCA, verificación y corrección:
    - Verificamos que las actividades declaradas pueden contener todas las aplicaciones informáticas y actividades tratamiento de datos personales realizadas por Eustat.

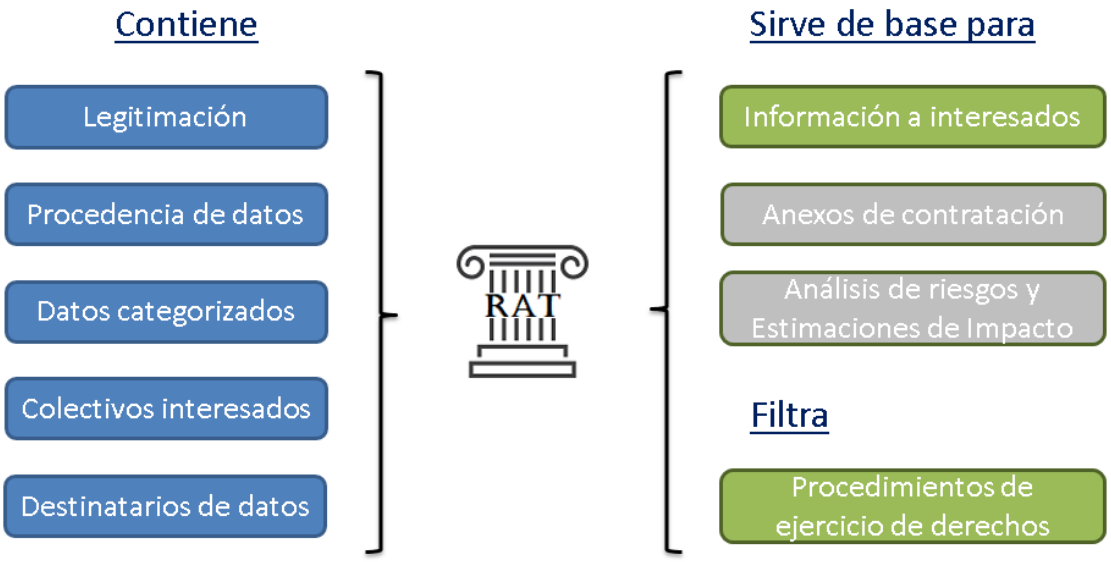
        - Verificamos que el RAT propone una información comprensible de lo que hace Eustat para el ciudadano.
        - Se propone a la Delegada de Protección de Datos para su publicación en el RAT de Gobierno Vasco:
            - Cambios de nomenclatura.
            - Cambios en la categorización de las actividades.
    - **Obtención del RAT versión 2 (RATv2).**

3.2. Proceso de estandarización.

- Privacidad por defecto y desde el diseño
    - Embeber la privacidad en el diseño de las operaciones estadísticas.
        - Rellenar obligatoriamente el modelo de datos personales que se recogen en cada operación.
    - Protección a lo largo de todo el ciclo de vida.
        - Actualización de la hoja Excel y comunicación por cada cambio que se produzca en el diseño de operación.
    - Valorar la privacidad, por defecto.
        - Revisión, por parte de la dirección, de la hoja Excel, que cumpla los principios de tratamiento de datos personales (minimización, …).
    - Enfoque ciudadano y transparencia.
        - Mostrar en el RAT la mayor cantidad de información.
        - Comunicación clara del ejercicio de derechos.
- Aseguramiento del cumplimiento.
    - Realizar cambios en los procedimientos de calidad sujetos a ISO 9001 para contemplar en el diseño de operaciones estadísticas (modificación o creación) el tratamiento de datos personales:
        - Añadir modelo para registrar los tratamientos de datos personales.
    - Auditoría periódica interna de cumplimiento LOPDGDD.
        - Conocimiento por parte de la dirección del nivel real de implantación.

4. Conclusiones.

- **El RAT pilar de la protección de datos**



- Información a interesados (clausulas informativas)
  - Ejemplo de Generación automática del clausulado informativo, a partir de la actividad de tratamiento "Encuesta de población en relación con la actividad" del RAT.
  - Capa 1:

Información sobre protección de datos

Sede electrónica

Información básica sobre protección de datos

Sus datos de carácter personal serán tratados e incorporados a la actividad de tratamiento denominada: *Encuesta de población en relación con la actividad.*

- **Responsable**: EUSTAT
- **Finalidad**: Producción de información estadística continua sobre la participación de la población en la actividad económica. Es el equivalente a la Labour Force Survey de la Unión Europea.
- **Legitimación**:
  - Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- **Destinatarios:**
  - Instituto Nacional de Estadística
  - Miembros de la Organización Estadística de la Comunidad Autónoma de Euskadi
- **Derechos**: Usted tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos que se recogen en la información adicional.
- **Información adicional**: Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web: www.euskadi.eus/clausulas-informativas/web01-sedepd/es/transparencia/140600-capa2-es.shtml

Normativa:

- Reglamento General de Protección de Datos (eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (www.boe.es/buscar/doc.php?id=BOE-A-2018-16673)

  - Capa 2:

Información sobre protección de datos

Encuesta de población en relación con la actividad

¿Quién es el responsable del tratamiento de sus datos?

EUSTAT

Donostia-San Sebastián 1, 01010, Vitoria-Gasteiz, Álava

Teléfono: 945017500

Página web: http://www.eustat.eus

Delegada de protección de datos

Donostia-San Sebastián 1, 01010, Vitoria-Gasteiz, Álava

Teléfono: 945 018 680

Página web: www.euskadi.eus/proteccion-datos

¿Con qué finalidad tratamos sus datos personales?

Detalle de la finalidad

Producción de información estadística continua sobre la participación de la población en la actividad económica. Es el equivalente a la Labour Force Survey de la Unión Europea.

¿Cuál es la legitimación para el tratamiento de sus datos?

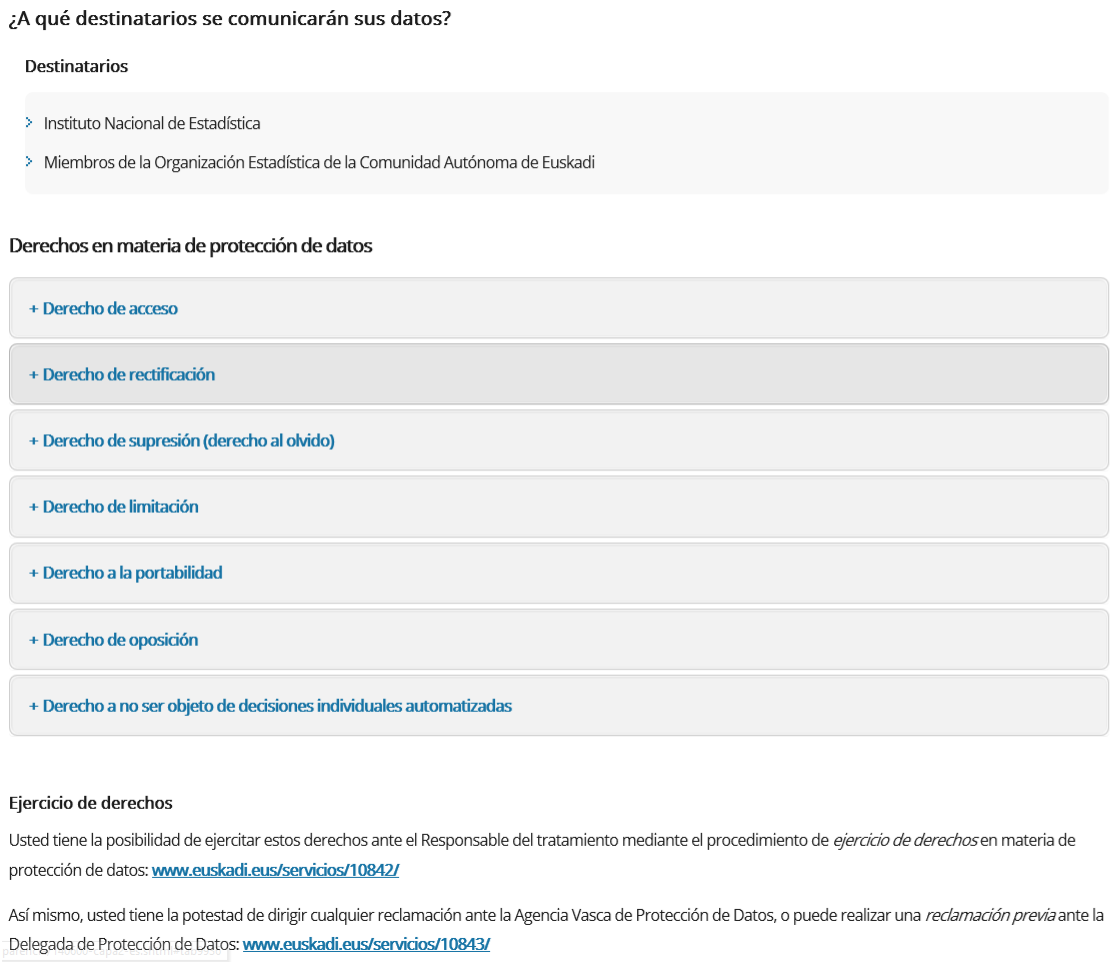
Legitimación

- Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- Ley 4/1986, de 23 de abril, de Estadística de la Comunidad Autónoma de Euskadi.
- Ley 8/2019, de 27 de junio, del Plan Vasco de Estadística 2019-2022.

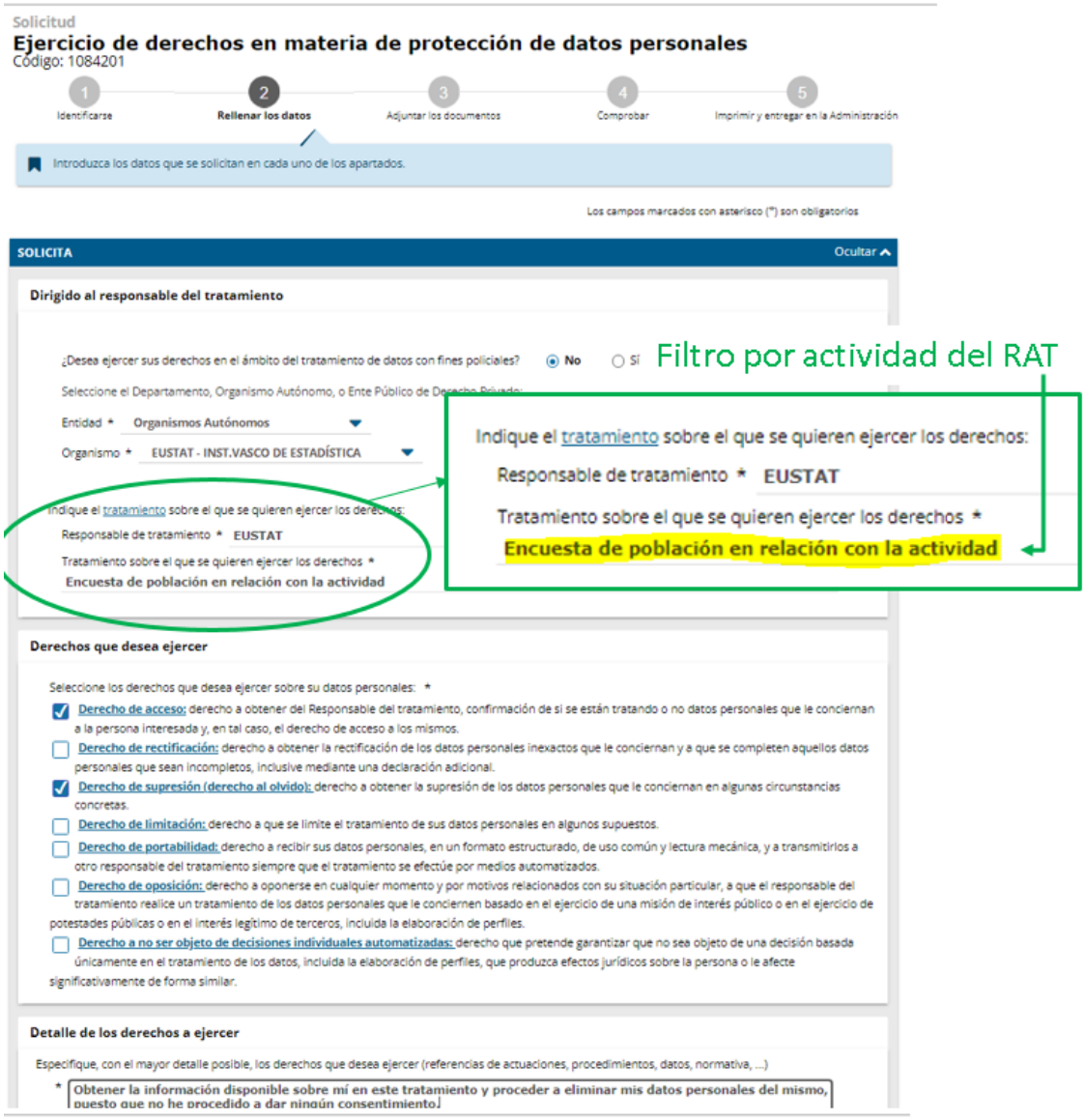
¿Por cuánto tiempo se conservarán sus datos?

Plazo de conservación de los datos

Tiempo que es necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades. Será de aplicación lo dispuesto en la normativa de archivos y documentación.



- Ejemplo de uso del RAT en el ejercicio de derechos ARCOPOL para la actividad de tratamiento “Encuesta de población en relación con la actividad” del RAT.


Solicitud
Ejercicio de derechos en materia de protección de datos personales
Código: 1084201
1 Identificarse
2 Rellenar los datos
3 Adjuntar los documentos
4 Comprobar
5 Imprimir y entregar en la Administración
Introduzca los datos que se solicitan en cada uno de los apartados.
Los campos marcados con asterisco (*) son obligatorios
SOLICITA
Ocultar
Dirigido al responsable del tratamiento
¿Desea ejercer sus derechos en el ámbito del tratamiento de datos con fines policiales? No Sí
Seleccione el Departamento, Organismo Autónomo, o Ente Público de Derecho Privado:
Entidad * Organismos Autónomos
Organismo * EUSTAT - INST.VASCO DE ESTADÍSTICA
Indique el tratamiento sobre el que se quieren ejercer los derechos:
Responsable de tratamiento * EUSTAT
Tratamiento sobre el que se quieren ejercer los derechos *
Encuesta de población en relación con la actividad
Filtro por actividad del RAT
Indique el tratamiento sobre el que se quieren ejercer los derechos:
Responsable de tratamiento * EUSTAT
Tratamiento sobre el que se quieren ejercer los derechos *
Encuesta de población en relación con la actividad
Derechos que desea ejercer
Seleccione los derechos que desea ejercer sobre su datos personales: *
Derecho de acceso: derecho a obtener del Responsable del tratamiento, confirmación de si se están tratando o no datos personales que le conciernan a la persona interesada y, en tal caso, el derecho de acceso a los mismos.
Derecho de rectificación: derecho a obtener la rectificación de los datos personales inexactos que le conciernan y a que se completen aquellos datos personales que sean incompletos, inclusive mediante una declaración adicional.
Derecho de supresión (derecho al olvido): derecho a obtener la supresión de los datos personales que le conciernan en algunas circunstancias concretas.
Derecho de limitación: derecho a que se limite el tratamiento de sus datos personales en algunos supuestos.
Derecho de portabilidad: derecho a recibir sus datos personales, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento siempre que el tratamiento se efectúe por medios automatizados.
Derecho de oposición: derecho a oponerse en cualquier momento y por motivos relacionados con su situación particular, a que el responsable del tratamiento realice un tratamiento de los datos personales que le conciernen basado en el ejercicio de una misión de interés público o en el ejercicio de potestades públicas o en el interés legítimo de terceros, incluida la elaboración de perfiles.
Derecho a no ser objeto de decisiones individuales automatizadas: derecho que pretende garantizar que no sea objeto de una decisión basada únicamente en el tratamiento de los datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre la persona o le afecte significativamente de forma similar.
Detalle de los derechos a ejercer
Especifique, con el mayor detalle posible, los derechos que desea ejercer (referencias de actuaciones, procedimientos, datos, normativa, ...)
* Obtener la información disponible sobre mí en este tratamiento y proceder a eliminar mis datos personales del mismo, puesto que no he procedido a dar ningún consentimiento