

RGPD

ITAPP

Hoja de control

| | | | |
|------------------------|---|----------------------------|----------|
| Organismo | Equipo de desarrollo del producto ITAPP | | |
| Proyecto | ITAPP | | |
| Entregable | RGPD | | |
| Autor | Haritz Saiz, Xabier Gandiaga, Álvaro Huarte, Xabier Etxezarreta, Onintza Ugarte y Ander Bolumburu | | |
| Versión/Edición | 0001 | Fecha Versión | 30/05/20 |
| Aprobado por | | Fecha Aprobación | 08/06/20 |
| | | Nº Total de Páginas | 8 |

REGISTRO DE CAMBIOS

| Versión | Causa del Cambio | Responsable del Cambio | Fecha del Cambio |
|---------|------------------|------------------------|------------------|
| 0100 | Versión inicial | Ander Bolumburu | 25/05/20 |
| | | | |
| | | | |

CONTROL DE DISTRIBUCIÓN

| Nombre y Apellidos |
|------------------------|
| Ander Bolumburu Casado |
| |
| |
| |
| |

Índice

| | | |
|-------|---|---|
| 1. | Introducción..... | 3 |
| 1.1 | Tratamiento de datos personales..... | 3 |
| 1.1.1 | Por qué considerar estos datos, datos anonimizados..... | 4 |
| 1.2 | Tratamiento de datos no personales..... | 5 |
| 1.3 | Otras cuestiones..... | 5 |
| 1.3.1 | Escenarios a tomar en cuenta..... | 6 |
| 1.3.2 | Evaluación de impacto | 7 |
| 1.4 | Consideraciones de licencias..... | 7 |
| 1.4.1 | Licencias de uso de APIs | 7 |

1. Introducción

Uno de los recursos más claves de cualquier empresa es la información o datos de la que disponen. A la hora de hablar sobre todos los datos que dispone la empresa, se manejan datos de diversa naturaleza categorizables en dos grupos establecidos en la RGPD: Datos personales, y no personales. Aquellos datos, entre otros criterios, que permitan identificar a personas físicas de manera inequívoca, son etiquetados como datos personales. Por el contrario, y con muchas salvedades, se consideran datos no personales.

Desde este punto de vista, nuestra empresa elabora el presente informe donde se pretenden recoger e identificar todos los datos con los que trabaja nuestra empresa y categorizarlo en uno de esos dos grandes grupos. Además, se aportarán todas aquellas consideraciones que se estimen oportunas para enriquecer cualquiera de los aspectos que se deban tener en cuenta para cumplir con dicha normativa.

1.1 Tratamiento de datos personales

Como el principal valor diferencial de nuestra empresa se basa en ofrecer el servicio de un modelo de Deep Learning, uno de los principales activos son los datos con los que enriquecer el mismo.

Es por ello por lo que ITAPP trata con muchos datos de carácter personal. A continuación, listaremos todos aquellos datos personales que son almacenados temporalmente (de forma previa a la anonimización los datos sí que existen de manera personal en nuestro sistema) o tratados por nuestros sistemas:

- Todos aquellos datos o textos que hagan referencia a una persona en concreto serán consideradas personales, ya sean diferentes tweets o incluso imágenes en las que aparezcan las personas usuarias, etc.

Dicha información se obtiene sin la previa autorización de los usuarios, pero al hacer uso de la red social, el usuario está pidiendo que esa información se divulgue, siendo esta captada a través de la API tal y como se referencia en [este link](#). El caso es el mismo con las demás redes sociales utilizadas.

Esos datos jamás son utilizados con ningún otro fin que alimentar el modelo de inteligencia artificial con la finalidad de que sea capaz de afrontar una mayor variedad de situaciones, haciendo mejor nuestro producto.

Todo dato que se almacena en nuestros sistemas con este fin es anonimizado puesto que se descarta la información referente al usuario que publicase el post en cuestión, imposibilitando la posterior unión entre usuario y dato.

- Por último y no menos importante, cualquier información que no se haya recogido con anterioridad y que recoja información de carácter personal según la RGPD jamás será utilizada sin previo consentimiento de dicha persona.

En ninguna circunstancia se realizará ni captarán datos personales si no se dispone de un consentimiento afirmativo por parte de la persona/fuente en cuestión. Su silencio omiso implicará que no está conforme con la captación de esos datos y por tanto no se podrán procesar o captar. Cualquier consentimiento será registrado con el fin de demostrar que el usuario autorizó dicha captación o procesamiento.

En cualquier momento nuestros usuarios podrán solicitar la eliminación de cualquier dato de tipo personal.

Una vez los datos son anonimizados dejan de ser datos personales.

https://protecciondatos-lopd.com/empresas/seudonimizacion-anonimizacion/#Anonimizacion_o_disociacion_de_datos_personales

1.1.1 Por qué considerar estos datos, datos anonimizados

¿Por qué considera Itapp que las publicaciones de los usuarios con una cantidad de datos descartada, como pueden ser el timestamp de la publicación, la cuenta de donde proviene, la IP de donde proviene la publicación etc. son datos anonimizados?

Los datos se consideran anónimos y no personales si estos no se pueden volver a reidentificar con las personas a las que pertenecen. En un principio debería de ser posible el escoger una publicación y buscar esa misma publicación en las redes sociales que Itapp utiliza como fuente.

Sin embargo, existe la posibilidad de que varias personas hayan generado una publicación parecida o exactamente igual, ya sea por algo como un retweet (que haya sido lo que hayamos consumido, que no el tweet original), hayan copiado y pegado la publicación o simplemente se haya dado la casualidad de que lo hayan acertado por completo.

Es verdad que esto no es el escenario más común, pero puede llegar a darse. En Itapp consideramos una defensa válida el escudarnos en esto para describir los datos que utilizamos como anonimizados y no personales.

1.2 Tratamiento de datos no personales

ITAPP también hace uso de datos no personales, esto incluiría publicaciones de carácter no personal en redes sociales (posts profesionales divulgativos, anuncios, posts de otros bots, etc.). Dicha información será usada con el mismo fin que los datos personales, es decir, alimentar la red neuronal.

Hablando de los datos personales, una vez estos son anonimizados descartando la información referente a la persona que los publicó, estos se convierten en datos no personales.

Un aspecto recogido según la RGPD, es que no se pueden poner prohibiciones en cuanto a la recolecta, guardado y perseverancia de los mismos.

1.3 Otras cuestiones

ITAPP debe de tener un responsable de tratamiento, responsable que se registrará por el cumplimiento de un contrato jurídico que vincula el objeto, duración, tipo de datos personales, obligaciones y derechos del responsable.

Dicha persona deberá garantizar que cualquier persona que esté autorizada para el tratamiento de datos se comprometa a mantener la confidencialidad y otras cuestiones mediante un contrato.

Dicho contrato regulará y estipulará que cualquier encargado deberá, una vez los procesos de tratamiento de datos personales terminen, eliminar cualquier copia de dichos datos. Y por supuesto, facilitará la realización de auditorías, inspecciones por autoridades u otro personal autorizado por el responsable de tratamiento.

También será el encargado de supervisar el procedimiento de anonimización por descarte y comprobar que este satisfactoriamente transforma los datos de carácter personal a no personal.

Al no superar los 250 empleados, pero si realizar tratamiento de datos personales de manera habitual, la RGPD recoge que es necesario llevar un registro de toda la actividad de tratamiento.

Dicho registro deberá incluir dos partes:

- **Responsable:** El nombre del responsable, fines del tratamiento, que en este caso sería preprocesar los datos con el fin de alimentar el modelo de inteligencia artificial, descripción de las categorías de datos personales, descripción de medidas de seguridad adoptadas y anonimización de dichos datos.
- **Encargado de tratamiento:** Nombre del encargado, y de todos los responsables y del delegado de protección de datos. Que tipos de datos utiliza cada responsable, transferencias de datos a países u organizaciones internacionales y medidas de seguridad adoptadas

Con el fin de minimizar incidentes de seguridad o su repercusión ITAPP realiza un cifrado de todos los datos tanto personales como no personales en las comunicaciones, se intenta garantizar la confidencialidad, disponibilidad e integridad de los datos y se realizan procesos de evaluación de forma regular para valorar la eficiencia de las medidas técnicas.

En caso de brecha de seguridad se notificará en un plazo inferior a 72 horas a la agencia de protección de datos española AEPD del incidente detallando el número de personas afectadas y gravedad de esta.

Si la brecha afecta a datos de carácter muy sensible se realizará una comunicación directa con el afectado o un comunicado público.

1.3.1 Escenarios a tomar en cuenta

Se espera que el efecto de una brecha no sea demasiado grave puesto que los datos con los que trata ITAPP son publicaciones en redes sociales. El único escenario grave que se prevé es que publicaciones que posteriormente han sido borrados por la persona publicante se filtren de cara al público.

Esto podría significar la vuelta de contenido indeseado por el usuario a internet de una forma pública. De todas maneras, no creemos que esto tenga grandes consecuencias puesto que casi todas las publicaciones de redes sociales son accesibles una vez estos se han borrado por páginas que se dedican a archivar información borrada de internet, como pueden ser waybackmachine.org o páginas especializadas en almacenar cambios en una red social en concreto.

Las probabilidades de que esto ocurra tampoco son muy altas puesto que la anonimización de los datos ocurre de manera casi simultánea a su recogida.

1.3.2 Evaluación de impacto

En caso de que un dato personal se filtre desde Itapp o se incumpla con la RGPD las sanciones rondan entre un 4% del volumen del negocio anual a 20 millones de euros. Aparte de esto, una infracción de la RGPD puede significar la terminación indefinida del contrato con los proveedores de servicio por parte de los proveedores y la ordenación por parte de una autoridad con potestad legal en el ámbito de la seguridad de datos sobre las acciones a tomar por Itapp.

En resumen, una infracción de la RGPD puede terminar con uno o varios de estos escenarios siendo aplicados a Itapp:

1. Advertencias
2. Apercibimientos
3. Órdenes (cómo actuar)
4. La retirada de una certificación (ISO o cumplimiento de la RGPD)
5. Multas administrativas

Estos pueden obligar a que Itapp reajuste su tratamiento de datos a uno que cumpla mejor con la RGPD hasta la suspensión del uso de datos de manera indefinida.

1.4 Consideraciones de licencias

Cualquier software empleado por el personal de ITAPP deberá disponer de su pertinente licencia de uso. No se permite el uso de software de manera ilícita o “pirata” en ninguna circunstancia. En caso de no seguir con estas consideraciones, el empleado haciendo uso de dicho software será penalizado con un expediente sancionador y/o penalización económica.

1.4.1 Licencias de uso de APIs

Las claves de acceso para las APIs de las redes sociales explotadas por ITAPP son obtenidas a nombre de la empresa y puede ser utilizado por cualquiera de los encargados de tratamiento. El uso de dichas claves se atiene a los términos y condiciones de uso de las redes sociales y APIs a las que pertenecen.