EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS EN LAS APPS DE SALUD

Proyecto PG E-salud

ALUMNO: DAVID BENEDED BLÁZQUEZ

TUTOR: Dr. ISIDRE FÀBREGUES ALADREN

Universitat Oberta de Catalunya

Objetivos del trabajo

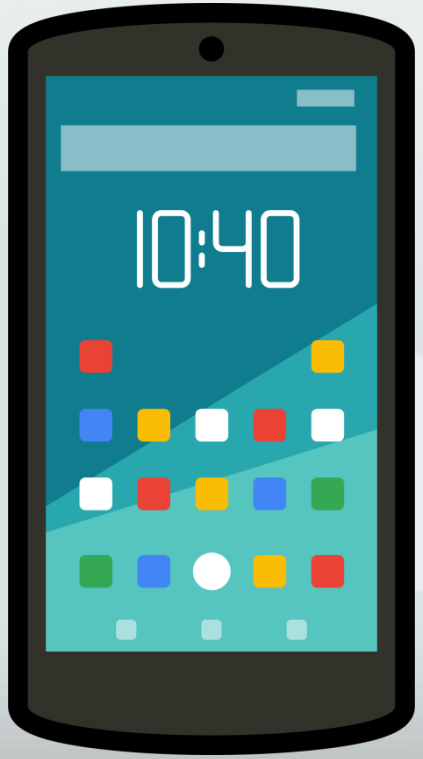
- Dar a conocer qué es la *mHealth* y las *apps de salud*
- Examinar sus beneficios y problemas: ¿existen riesgos para la seguridad, privacidad, confidencialidad e integridad de los datos personales de los usuarios que las manejan?.
- Determinar el marco normativo que le son aplicables en materia de protección de datos y otras leyes del ordenamiento jurídico español le afectan.
- Analizar los conceptos jurídicos básicos y principios fundamentales de la normativa vigente (el Reglamento General de Protección de Datos)
- Concienciar a los desarrolladores la transcendencia de cumplir con el RGPD
- Difundir una serie de recomendaciones y buenas prácticas

Universitat Oberta de Catalunya

Proyecto PG E-Salud

La *mHealth* y las aplicaciones móviles de salud

¿Qué es la *mHealth* o salud móvil?



- Hay **8.000 millones de teléfonos móviles**, un número mayor al de personas que hay en el mundo.
- Los teléfonos inteligentes o **smartphones** son los dispositivos más usados para acceder a Internet y han cambiado la forma de comunicarnos, informarnos, pasar el tiempo de ocio y, hasta de cuidar la salud.
- En este ámbito, surge la mHealth o salud móvil: “la práctica médica y de salud pública apoyada por dispositivos móviles, tales como teléfonos móviles, dispositivos de monitorización de pacientes, asistentes digitales personales (PDA) y otros dispositivos inalámbricos” (OMS, 2011).

Ilustración: Cartoon Android Smartphone (by openclipart.org)

Características principales de la *mHealth*

- **Accesibilidad**: ubicuidad, acceso universal en cualquier momento.
- **Personalización:** soluciones individualizadas para abordar las necesidades específicas.
- **Inmediatez**: servicios en el momento preciso con información pertinente, puntual y oportuna.
- **Interactividad**: promoviendo la cocreación y una interacción bidireccional intensa y a largo plazo
- **Movilidad**: temporal, espacial y contextual.
- **Localización**: proporcionando servicios específicos mediante sistemas de posicionamiento global.

Ilustración: Características principales de la mHealth según Akter, D'Ambra y Ray (2013)

Las *apps*, máximo exponente de la *mHealth*

- Ofrecen ubicuidad, facilidad de uso, versatilidad, multifuncionalidad, interactividad, sensibilidad al entorno e, incluso, su bajo o nulo coste para los usuarios
- Herramientas de comunicación, información y motivación: recordatorios de medicación, hábitos saludables.
- Interconexión con otros sistemas de información como la HCE.
- Monitorización mediante sensores y wearables de constantes vitales y una gran cantidad de datos médicos, fisiológicos, relativos al modo de vida y a la actividad diaria.

Ilustración: Grupo de Nuevas Tecnologías de la SoMaMFyC

Miles de *apps de salud* con multitud de funciones

Actualmente hay **259.00 *apps de salud*** en las principales tiendas, produciéndose en 2016 **3.000 millones de descargas** y previéndose que en 2020 haya **551 millones de usuarios**.

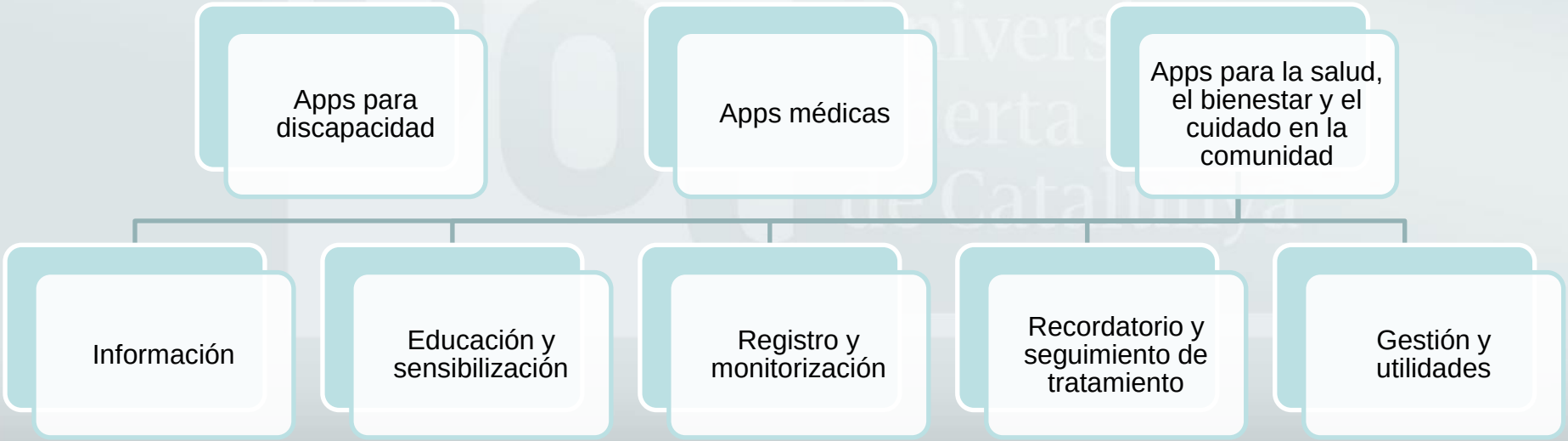
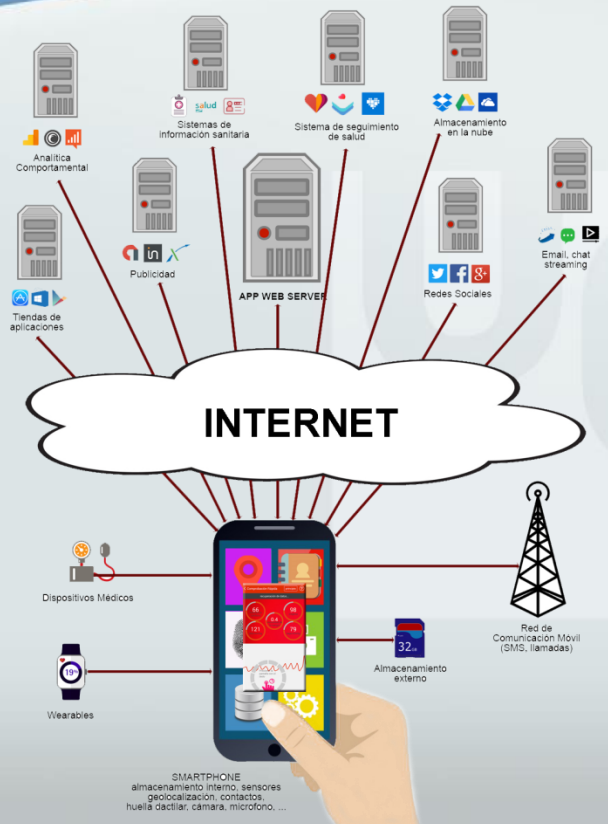


Ilustración: Categorizaciones de PatientView y The App Date

Variado ecosistema y compleja arquitectura

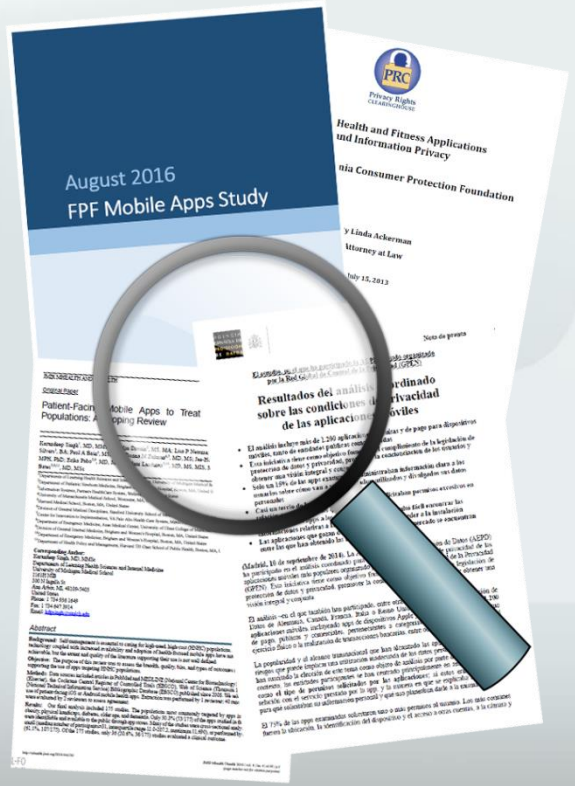


Las apps recopilan ingentes cantidades de datos personales

- Tiendas de aplicaciones para poderla descargar
- Datos introducidos por el usuario en la app para su registro y durante la utilización de la misma
- Datos automatizados procedentes de los sensores del propio dispositivo, o wearables interconectados vía Bluetooth
- Datos que se almacenan en varios servidores
- Conectividad con otros servidores para acceder a datos, hacer backups, envío de email, compartir en redes sociales
- Uso de herramientas para analítica de comportamiento

Ilustración: Arquitectura “tipo” de una app de salud

Revisión de la literatura científica



Sobre las 600 apps de salud más descargadas, el 69,5% no tenían políticas de privacidad y el 66% de las que si tenían no hacían en ella referencia específica a la misma sino a otros servicios.

(Sunyaev et al., 2014)

El 26% de las apps gratuitas y el 40% de las de pago, sin política de privacidad.

(Linda Ackerman, 2013)

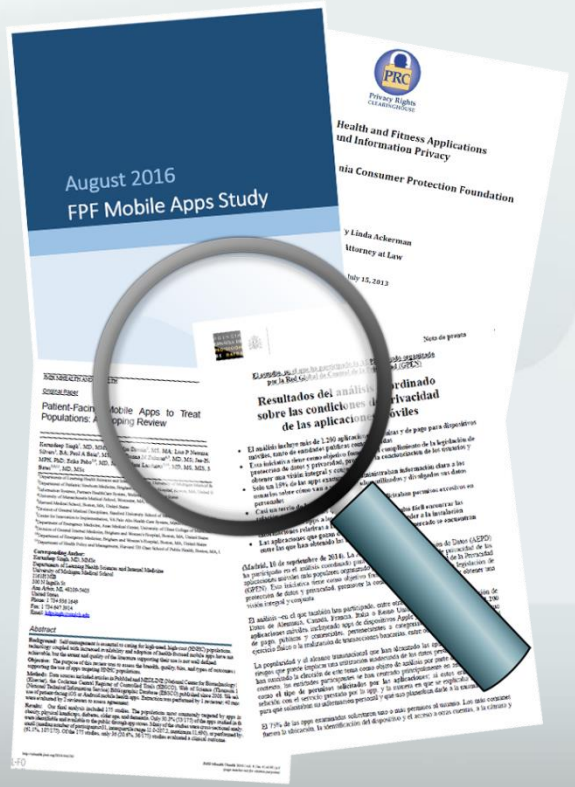
Un 15% de 1200 apps NO suministraban información clara a los usuarios sobre cómo iban a ser recopilados, utilizados y divulgados sus datos, y el 31% de las apps analizadas solicitaban permisos excesivos

(RGCP, 2014)

20 de las apps más populares transmitían datos a una red de 70 empresas.

(Financial Times, 2013)

Revisión de la literatura científica



*El 100% de las apps de la Health Apps Library de la NHB no cifraban los datos en local y el 66% tampoco lo hacían durante el transporte, lo que provocaría el cierre de la biblioteca hasta entonces "**modélica**".*

(Huckvale et al., 2015)

Solo el 19% de apps para la diabetes en Google Play tenían la política de privacidad accesible desde la propia tienda.

(Knorr et al., 2015)

El 86,2% de las apps para la diabetes en Android tenían cookies de rastreo sin notificarlo.

(Blenner et al., 2016)

Riesgos para la privacidad y seguridad de los datos

La revisión de la literatura científica pone de manifiesto que las apps de salud no suelen tratar adecuadamente los datos de sus usuarios o, al menos, **suponen un riesgo significativo para la privacidad y la seguridad** de dicha información, principalmente por tres causas:

- La ausencia de información transparente a los usuarios
- La maximización de los datos y multiplicidad de finalidades
- Las insuficientes y, en muchos casos, deficientes medidas de seguridad

Ilustración: Low Security Icon (by openclipart.org)

Universitat Oberta de Catalunya

Proyecto PG E-Salud

La normativa en materia de protección de datos aplicable a las *apps de salud*

El marco regulador en protección de datos

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental reconocido en la Carta de Derechos fundamentales de la Unión Europea (art. 18.1)

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.

Adaptación en España:

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de Desarrollo

Desde mayo de 2016 (y efecto desde el 25/05/2018)

Reglamento General de Protección de Datos

¿Se debe aplicar el RGPD a las *apps de salud?*

- Se aplica porque a través de las apps de salud se procede al registro, almacenamiento, acceso y tratamiento de datos de una persona física, directa o indirectamente, identificada o identificable, es decir, porque tratan **datos personales**.
- **Desde el momento que genera tráfico de datos personales** (se envían o almacenan datos a un servidor o se tiene acceso a los datos "en local") y los datos son tratados por un responsable del tratamiento (sea un programador individual, una organización pública o privada o cualquiera que determine las finalidades para las que se tratan dichos datos).
- **Se debe cumplir la normativa independientemente de donde resida el responsable**, ya que en el tratamiento intervienen personas y recursos (el propio dispositivo) en la UE.
- No resulta aplicable cuando no se registran datos personales, no se comparten con nadie ni sean tratados por el responsable del tratamiento ni por ningún otro tercero (por ejemplo, apps que no requieren registro pero que tampoco utilicen ningún medio de recolección automático como cookies).

Principios fundamentales del RGPD

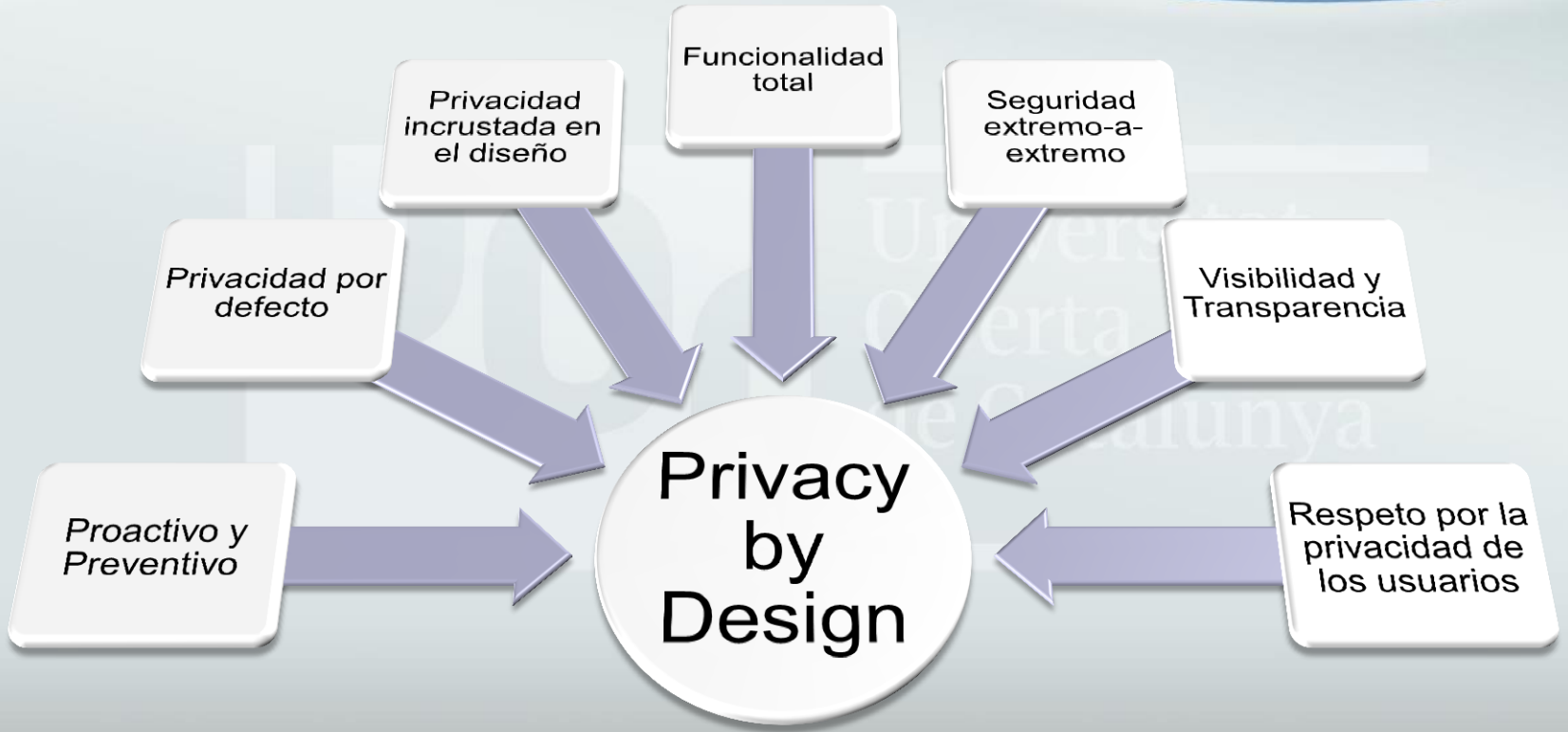

REGLAMENTOS

El RGPD estipula que los datos personales deben ser:

- Tratados de manera lícita, leal y transparente
- Recogidos con fines determinados, explícitos y legítimos
- No serán tratados ulteriormente de manera incompatible a esos fines
- Adecuados, pertinentes y limitados a lo necesario
- Exactos y actualizados
- Mantenidos durante no más tiempo del necesario
- Tratados con seguridad

El responsable del tratamiento se hace cargo del cumplimiento de estos principios debiendo ser capaz de demostrarlo (responsabilidad proactiva)

Principio de Privacidad desde el Diseño



Universitat Oberta de Catalunya

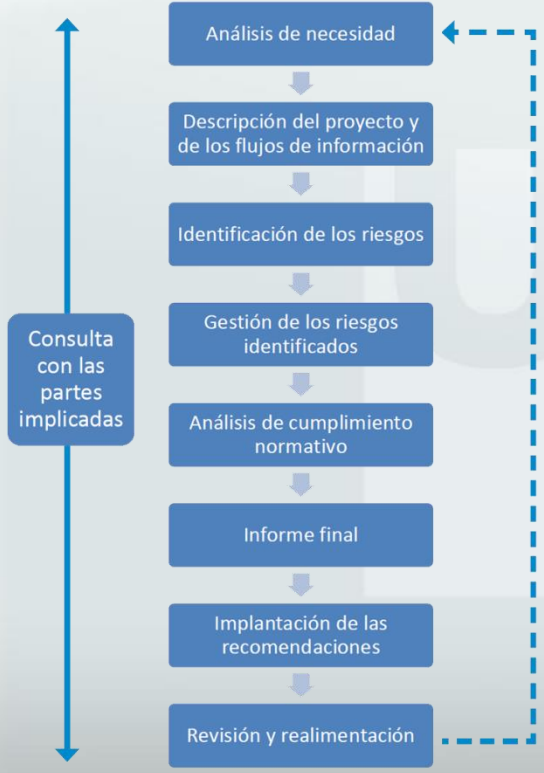
Proyecto PG E-Salud

Difusión de "buenas prácticas" para desarrolladores de *apps de salud*

Cumplimiento del RGPD desde la conceptualización

- Tener presente la privacidad y el cumplimiento de los requerimientos de la normativa de protección de datos **desde la propia conceptualización de la *app***
- Observar una serie de **obligaciones para con la autoridad competente.**
- Proceder a la **exhaustiva selección de los encargados de tratamiento** que ofrezcan garantías suficientes para aplicar las medidas técnicas y organizativas.
- **Regirse por un contrato** que vincule al encargado respecto al responsable
- Tenerlo muy presente en las relaciones con proveedores de servicios hosting y cloud computing ya que **se pueden considerar transferencias internacionales** sino se localizan sus recursos en el Espacio Económico Europeo. Especial precaución con empresas de Estados Unidos, debiendo estar adheridas al **Escudo de Privacidad**.
- Designación de **Delegado de Protección de Datos** (DPD)

Evaluación de Impacto de Protección de Datos

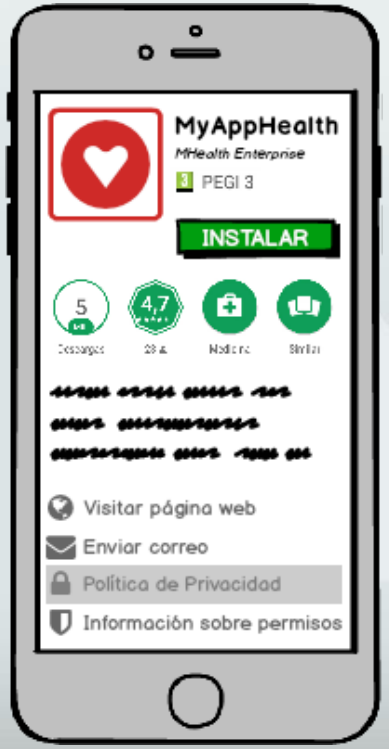


- La debe realizar el responsable del tratamiento, especialmente cuando se usen nTIC, **cuando sea probable que un tipo de tratamiento entrañe un alto riesgo** para los derechos y libertades de las personas físicas.
- EIPD es una **metodología para evaluar el impacto en la privacidad** tras haber consultado con todas las partes implicadas, tomar las medidas necesarias para evitar o minimizar los impactos negativos.
- Se debe realizar **durante la fase inicial**, antes de cualquier tratamiento pero **también cuando cambien** las categorías de datos recabados, fines previstos.
- Consta de 8 fases que se retroalimentan.

Acreditar el cumplimiento y transmitir confianza

- Puesto que con la adopción de la responsabilidad proactiva, ya no es suficiente con no incumplir la normativa, **se debe acreditar el cumplimiento del RGPD**.
- **Adaptar lo previsto y requerido por la LOPD** (información de la inscripción de ficheros, documento de seguridad, autorías), para las **nuevas obligaciones como el Registro de Actividades de Tratamiento**.
- Buena oportunidad para un **SGSI**, pudiendo obtener la certificación ISO 27001 que garantiza que la seguridad está gestionada correctamente.
- También se transmite confianza a los usuarios mediante otros procesos como:

Cumplir con el deber de informar al usuario



- Proporcionar información **antes de la instalación** facilitando un *link* a la Política de Privacidad colocada en la web corporativa.
- Ofrecer la información **al iniciarse por primera vez la *app***, antes de solicitar el consentimiento del usuario.
- El deber de información **implica lealtad y transparencia**
- Ofrecer la información **requerida por el RGPD**:
  - Identidad y los datos de contacto del responsable y del DPD
  - Fines del tratamiento y los intereses legítimos del responsable del tratamiento
  - Destinatarios (incluyendo si se prevén transferencias internacionales)
  - Plazo de conservación y si se proyectan tratamiento ulteriores
  - Cómo ejercer los distintos derechos y la existencia de decisiones automatizadas
- Facilitar la **información técnica que resulte pertinente** así como los mecanismos de seguridad que tiene implementados.

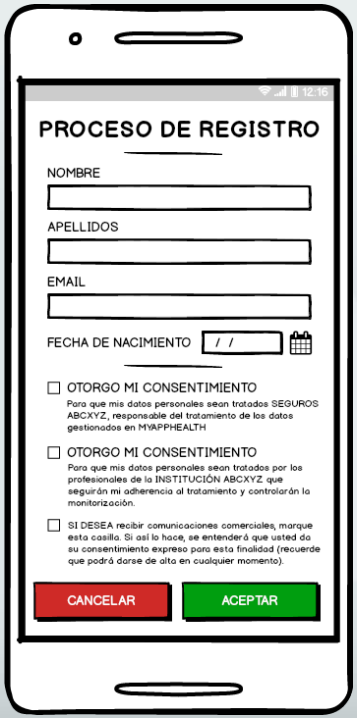
Cumplir con el deber de informar al usuario

- La información debe ser **fácil de entender**
- En un **lenguaje sencillo y claro**
- Presentarse **en forma concisa** y evitando un extenso y engorroso texto legal. Hay que evitar que el usuario se lo “salte”
- Proporcionar la información suficiente y útil **en los momentos adecuados** en los que se solicitan datos personales)
- Utilizar un formato de **varios niveles**
  - Primer nivel: de aviso breve y resumido
  - Segundo nivel: con toda la información completa aunque por apartados.
- Aplicando los **principios de diseño web adaptativo** y las **normas de Diseño Universal** (WCAG)

Obtener legitimización para el tratamiento

- Los tratamientos de los datos personales **deben estar legitimados** estableciéndose, en la mayoría de casos de este entorno, **el consentimiento del interesado como el único fundamento de legalidad** en el tratamiento de los datos personales de los usuarios de las mismas debiendo ser informado pero también libre, específico, inequívoco, explícito, demostrable, revocable.
- **LIBRE**: no se puede amedrentar ni asustar al interesado para que utilice la app ni tampoco es aceptable obligarle a proporcionar datos personales que no son estrictamente necesarios para la finalidad de la *app.*
- **INFORMADO**: ofreciéndose tras la “Política de Privacidad” y antes de iniciarse cualquier registro de datos. De forma sencilla y clara y separada de otros términos o de la EULA.
- **ESPECÍFICO**: no vale el consentimiento “para todo” sino granular y diferenciado para cada finalidad distinta a la funcionalidad prevista de la app incluyendo las recogidas de datos automatizados (por cookies y otros DARD) y excepto que sean técnicas.

Obtener legitimización para el tratamiento



- Promover la otorgación de **permisos expost** en tiempo de ejecución y en los momentos apropiados evitando darlos todos al inicio.
- **INEQUÍVOCO Y EXPLÍCITO:** Mecanismo de acción positiva no valiendo los silencios, casillas premarcadas ni las inacciones.
- Esforzarse para verificar la edad del usuario ya que se requiere que en caso de menores de 14 años (en España) haya sido dado por el titular de la patria potestad o tutor legal. Usar *Dni-e* o método COPPA.
- **DEMOSTRABLE**: mecanismos que permitan acreditar quién, cuándo, cómo y qué información se proporcionó (log's y doble opt-in).
- **REVOCABLE**: en cualquier momento y periódicamente renovarlo cuando haya actualizaciones o el usuario lleve tiempo sin usar la *app*.

Datos pertinentes, minimizados y exactos

- Los datos se deben obtener por **medios que no sean fraudulentos, leales y lícitos**
- Datos de calidad, es decir **adecuados, pertinentes y no excesivos** en relación con el ámbito y las finalidades determinadas, explícitas y legítimas determinadas para el tratamiento
- **Exactos**, con el menor número posible de términos en evitación de ambigüedades e imprecisiones, y **actualizados** de forma que respondan con veracidad a la situación actual.
- Especialmente importante en la recogida de datos a través de **wearables y por otros sensores**, como la geolocalización, debiéndose permitir elegir qué datos concretos de entre todos los que se ofrecen y durante cuánto tiempo.

Datos pertinentes, minimizados y exactos

- **Controles y sistemas de ayuda** en los formularios de entrada de datos **para evitar que se introduzcan datos erróneos o equivocados**.
- Aplicar los **principios heurísticos de usabilidad de Jakob Nielsen**

1) Visibilidad del estado del sistema
2) Correspondencia entre sistema y mundo real
3) Libertad y control por parte del usuario
4) Consistencia y estándares
5) Prevención de errores.
6) Reconocer antes que recordar
7) Flexibilidad y eficiencia en el uso
8) Diseño estético y minimalista
9) Diagnosticar y recuperarse de los errores
10) Ayuda y documentación

- Mecanismos para que los datos sean **introducidos una única vez** evitando duplicidades o que se pierdan accidentalmente **y posibilitando que los usuarios puedan modificarlos**.

Implementar medidas de seguridad adecuadas

- Tanto el responsable como el encargado del tratamiento aplicarán **medidas técnicas y organizativas apropiadas** para garantizar un nivel de seguridad adecuado al riesgo
- Los desarrolladores deben seguir **guías y metodologías expresamente dedicadas al desarrollo seguro** de aplicaciones para *smartphones*
- Se ha de ser **proactivo y preventivo**, anticipando y previniendo los riesgos desde el mismo diseño los posibles riesgos de seguridad. Se puede seguir, por ejemplo el **OWASP Top 10 Mobile Risk** para detectar los principales riesgos y usar la **Smartphone Secure Development Guidelines** para poner las medidas.
- Usar herramientas de desarrollo comunes; evitar el código complejo, elegir las bibliotecas de terceros más confiables; almacenar los datos de forma segura en un servidor.
- Seguridad también en la fase de testeo, publicar en tiendas oficiales y garantizar el mantenimiento con instalaciones correctas de actualizaciones y parches.

Implementar medidas de seguridad adecuadas

- Los datos personales deben estar **protegidos en cualquier momento y lugar** constituyéndose el cifrado como el medio idóneo.
- Para el almacenamiento seguro de los datos, parece recomendable implementar AES (**Advanced Encryption Standard**).
- Comunicaciones por la red seguras, mediante el protocolo TLS (**Transport Layer Security**), sucesor avanzado de SSL.
- Implementar un **sistema de autenticación de doble factor** (2FA).
- Establecer **políticas de contraseñas seguras**.
- **Cerrar sesiones** tras un tiempo sin interactividad y, **evitar los login persistentes** (proteger los identificadores de sesión).
- Para datos de salud, no parece adecuado *social login*

Implementar medidas de seguridad adecuadas

- Las medidas requeridas por el RGPD **refieren a todos los sistemas y servicios de tratamiento** y, por lo tanto, no se limitaría a la app de salud sino a toda la infraestructura que utilice, principalmente, al back-end y a los sistemas de información que tratan los datos personales recabados por la misma.
- Proteger **servidores** y controlar los tratamientos desde los sistemas de información
- La **anonimización y seudonimización**, deben ser vistas **como medidas de seguridad válidas y efectivas** para los tratamientos ulteriores y conservaciones de datos requeridas, y no como técnicas a emplear para evitar el cumplimiento normativo.
- En caso de producirse **violaciones de seguridad de los datos personales**, seguir un protocolo de actuación que requiere la **notificación a la autoridad de control** pertinente siendo recomendable dar aviso **a los interesados afectados**, aunque el RGPD prevea no notificarlo en algunos casos

Facilitar a los usuarios el ejercicio de sus derechos

- Implantar opciones en la propia *app* para ejercer los derechos directamente, cumplimentando **formularios ya estructurados**.
- Incluir **en el apartado de F.A.Q.** una explicación de cada uno de los derechos, incluyendo las restricciones en el RGPD y otras leyes.
- Aprovechar el entorno tecnológico para **implementar opciones automatizadas** que permitan al usuario tener conocimiento sobre el tratamiento llevado a cabo sobre sus datos personales sin que llegue a iniciarse el proceso administrativo de ejercicio de los derechos.
- Por ejemplo, en el ejercicio del derecho de acceso, **incluir un listado de los tratamientos llevados a cabo** y de los accesos que se han producido a los datos por parte del personal del responsable del tratamiento, encargados del mismo y por terceros.

Facilitar a los usuarios el ejercicio de sus derechos

- Facilitar la **obtención automática de una copia de los datos** a través de la exportación a formatos abiertos TXT o PDF (derecho distinto al de portabilidad).
- **Ejercer el derecho de supresión al desinstalar** la app, aunque se han de **prever las excepciones previstas** en el RGPD y por otras leyes sanitarias (LGS, LBAP) que llevarían a bloquearlos o trasladarlos a otro sistema.
- Utilización de **estándares de interoperabilidad** “sanitarios” para el derecho de portabilidad: datos de HCE (HL7 CDA, OpenEHR), dispositivos médicos (x73), imagen médica (DICOM).
- Contribuir a **concienciar al usuario sobre el valor que tienen sus datos personales** y la importancia de que ellos mismos (y no sólo los responsables de los tratamientos) empiecen a protegerlos.

Universitat Oberta de Catalunya

Conclusión Final

Los desarrolladores debemos tomar conciencia de la transcendencia que tiene el garantizar el cumplimiento de la normativa sobre privacidad y protección de datos y de la relevancia, incluso para el propio negocio, de transmitir confiabilidad en todo momento y a todo el mundo viendo esta obligación, no sólo como una imposición legal, sino como una oportunidad de mejorar nuestras soluciones centrándonos en el usuario en todos los aspectos.

¡Muchas gracias!