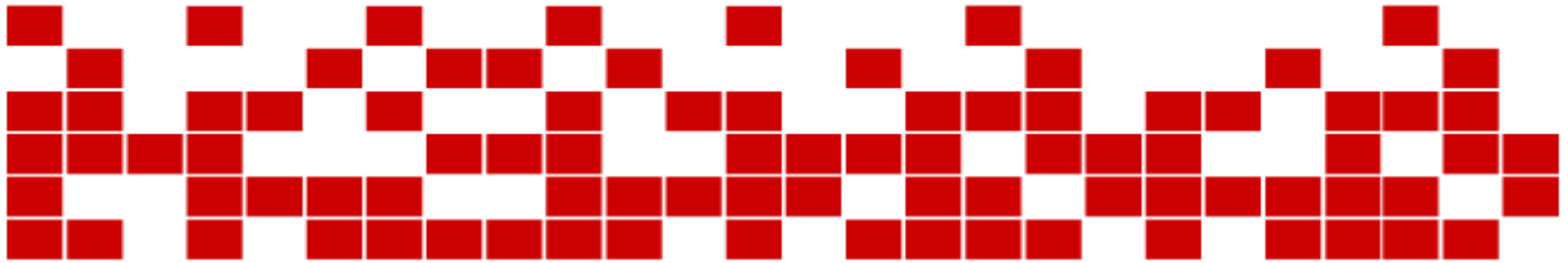
ISACA®
Trust in, and value from, information systems
Barcelona Chapter

NEOLEGIS

El Reglamento General de Protección de Datos: Retos y Oportunidades



ÍNDICE DE ASPECTOS A TRATAR

1. INTRODUCCIÓN: LA IMPORTANCIA DEL REGLAMENTO
2. ÁMBITO DE APLICACIÓN
3. PRINCIPIOS Y DERECHOS
4. “PERSONAJES” DEL REGLAMENTO

NEOLEGIS

ÍNDICE DE ASPECTOS A TRATAR

5. PRIVACIDAD DESDE EL DISEÑO Y PRIVACIDAD POR DEFECTO, EL REGISTRO

6. SEGURIDAD DEL TRATAMIENTO, NOTIFICACIONES Y EVALUACIONES DE IMPACTO

7. CÓDIGOS DE CONDUCTA Y CERTIFICACIONES

NEOLEGIS

ÍNDICE DE ASPECTOS A TRATAR

1. INTRODUCCIÓN: LA IMPORTANCIA DEL REGLAMENTO

NEOLEGIS

¡HABEMUS REGLAMENTO!

I

(Actos legislativos)

REGLAMENTOS

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 27 de abril de 2016

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

….¡Y PELÍCULA!

The Guardian
14.11.15

Democracy: the film that gets behind the scenes of the European privacy debate

¿POR QUÉ ERA TAN IMPORTANTE APROBAR EL RGPD?

1. REGULACIÓN DESFASADA ANTE EVOLUCIÓN TECNOLÓGICA

CONSEJO EUROPA

- Convenio Europeo de Derechos Humanos (1950)
- Convenio 108

UE

- Carta Dchos Fundamentales
- 16.2 TFUE
- Directiva 95/46/CE

ESPAÑA

- 18.4 CE
- LOPD y RLOPD

DESEQUILIBRIO TITULARES DE DATOS/TRATADORES: LAS TIC OTORGAN MÁS PODER EN NOMBRE DE:

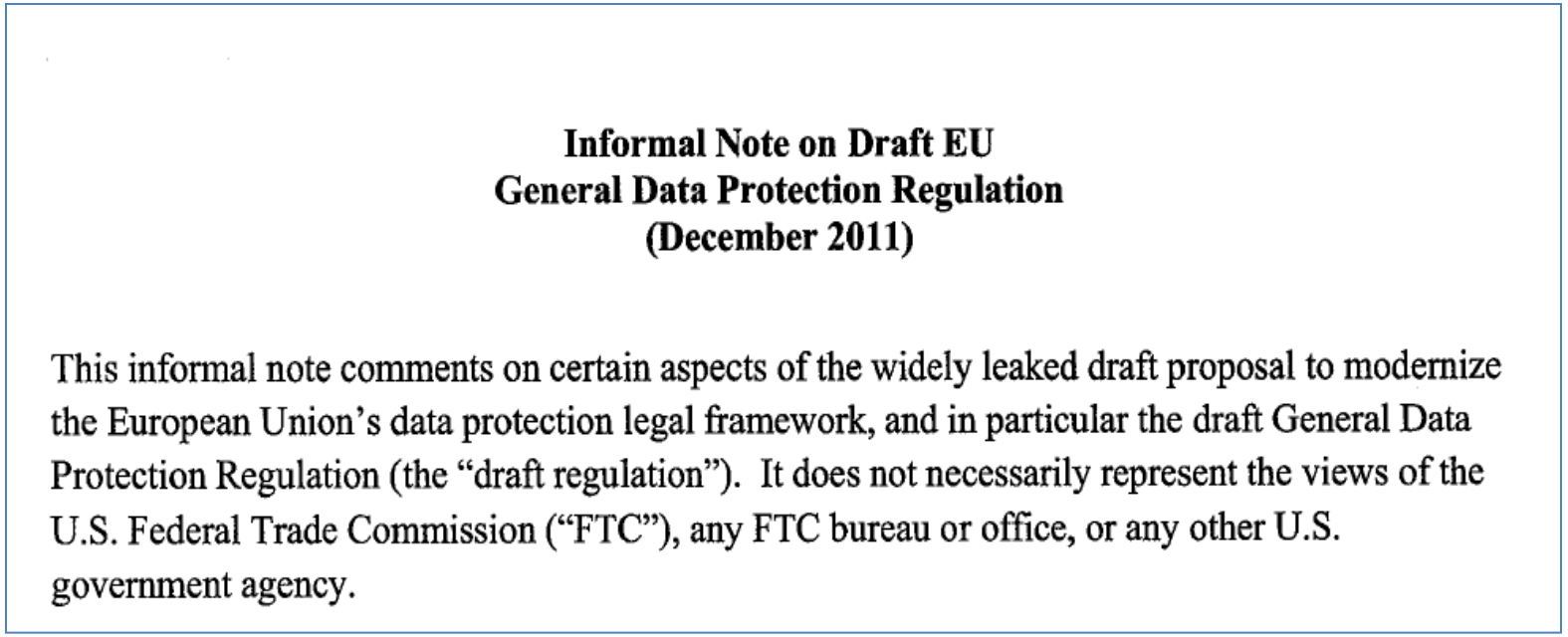
- ECONOMÍA (CRISIS)
- SEGURIDAD (TERRORISMO)
- TRANSPARENCIA (CORRUPCIÓN)
- INNOVACIÓN, CIENCIA (CURAR ENFERMEDADES)

2. ARMONIZACIÓN INSUFICIENTE

- 28 ESTADOS MIEMBROS, 28 LEGISLACIONES DIVERGENTES

RGPD: UN CAMINO DIFÍCIL

- Proceso legislativo: Enero 2012-Mayo 2016
- Lobbies (empresas Internet, gobierno EEUU…)
- Mientras… STJUE casos Google, Safe Harbour, filtraciones espionaje…



Informal Note on Draft EU
General Data Protection Regulation
(December 2011)

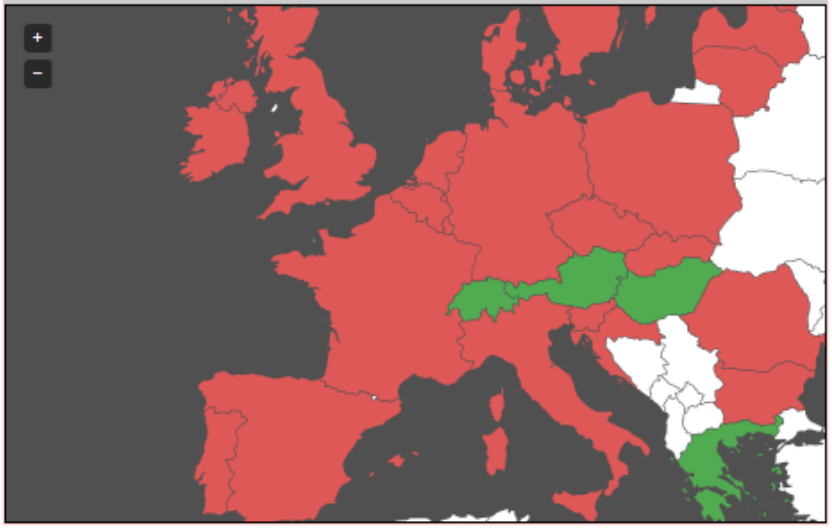
This informal note comments on certain aspects of the widely leaked draft proposal to modernize the European Union's data protection legal framework, and in particular the draft General Data Protection Regulation (the "draft regulation"). It does not necessarily represent the views of the U.S. Federal Trade Commission ("FTC"), any FTC bureau or office, or any other U.S. government agency.

LobbyPlag

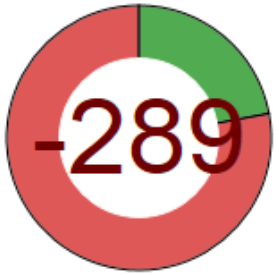
LobbyPlag 1 - Lobby&Paste LobbyP

Ranking Proposal Leaks Major Issues Governm

Countries



Overview Council



114 pro privacy
403 against

LobbyPlag.eu obtained about 11.000 pages of *classified* EU documents and a number of *classified* German diplomatic cables on the EU data protection reform. In addition to publishing many of the documents, LobbyPlag.eu also shows which national governments are working on lowering or raising data protection laws in Europe.

Countries/Politicians AGAINST

Countries/Politicians PRO

RGPD: UN REGLAMENTO EUROPEO

- Consecuencias de la utilización del instrumento jurídico:
  - 1 SOLA NORMA PARA LOS 28 EM. Objetivo: facilitar el cumplimiento
  - Desplazamiento normativa nacional…
  - …Aunque finalmente se ha dejado en muchos casos margen de maniobra a los Estados Miembros
  - Además la propia transversalidad de la regulación de protección de datos implica tener en cuenta (p.ej. para legitimación) la legislación nacional

RGPD: FECHAS CLAVE

FECHA DE PUBLICACIÓN	**4.5.2016**
FECHA DE ENTRADA EN VIGOR	**25.5.2016**
FECHA DE APLICACIÓN	**25.5.2018**

- A partir fecha de aplicación:
  - Es cuando habrá que cumplir el RGPD
  - Es cuando tiene efecto derogación Directiva 95/46/CE
  - Validez de consentimientos, decisiones y autorizaciones de Comisión y AC más allá de esa fecha

RGPD: OBJETIVOS Y AVANCES

OBJETIVOS:

- Protección de derechos fundamentales en un entorno tecnológico: “el tratamiento de datos debe servir a la humanidad”
- Garantizar la libre circulación de datos personales en la UE facilitando el cumplimiento a los sujetos obligados (RT y ET) con una sola norma

AVANCES

- Reconocimiento DCHO PROT DATOS: autónomo e instrumental que debe conjugarse con otros DF
- Cambio enfoque obligaciones: gobierno, autorresponsabilidad

ÍNDICE DE ASPECTOS A TRATAR

2. ÁMBITO DE APLICACIÓN

NEOLEGIS

ÁMBITO APLICACIÓN MATERIAL

- RGPD, sin cambios respecto a Directiva, **se aplica a**:
  - Tratamiento total o parcialmente automatizado de datos personales
  - Tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero
- **Exclusiones** también se mantienen, como la referida a actividades puramente personales o domésticas
- Se protege a **personas físicas**, no fallecidas ni jurídicas ni datos de contacto, como en normativa española.
- Concepto **dato personal**: inclusión identificadores, criterios para saber cuando una persona es identificable. Incentiva uso pseudónimos

ÁMBITO APLICACIÓN TERRITORIAL
COMPARATIVA LOPD/RGPD

LOPD	RGPD
Tratamiento efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento ubicado en España, o, Si hay un encargado del tratamiento se le aplicará Título VIII RLOPD	Se añade establecimiento del encargado del tratamiento y que será indiferente si el tratamiento tiene lugar en la UE o no
Aplicación en virtud Derecho internacional público	=
Responsable ubicado fuera UE que recurra a medios situados en territorio español, excepto si es con fines de tránsito	Responsable o encargado del tratamiento **ubicados fuera UE** cuando traten datos de individuos ubicados en UE: • **para la oferta de bienes o servicios**, aunque no impliquen pago • **Para el control de su conducta,** cuando esta conducta se lleve a cabo en la UE

ÍNDICE DE ASPECTOS A TRATAR

3. PRINCIPIOS Y DERECHOS

NEOLEGIS

PRINCIPIOS

COMPARATIVA LOPD/RGPD

LOPD	RGPD
Calidad	Licitud, lealtad y transparencia Limitación de finalidad Minimización Exactitud Limitación conservación
Información	Transparencia. También incluido en parte derechos
Consentimiento	Licitud
Datos especialmente protegidos	Categorías especiales de datos
Seguridad, Secreto	Integridad y Confidencialidad
Comunicación de datos	**NO**
Acceso a datos por cuenta de terceros	Obligación del responsable: Encargado Tratamiento
NO	**Accountability (rendición de cuentas)**

Accountability: Principle intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities." Supervisor Europeo de Protección de Datos

DERECHOS

COMPARATIVA LOPD/RGPD

LOPD	RGPD
Acceso	Acceso
Rectificación	Rectificación
Cancelación	Supresión (**olvido**)
Oposición	Oposición
Consulta Registro	**NO**
Impugnación de valoraciones	No sujetarse a una decisión automatizada (**profiling**)
Indemnización	Indemnización
Incluido en parte principios	Información
NO	**Portabilidad**
Bloqueo	Limitación del tratamiento

ÍNDICE DE ASPECTOS A TRATAR

4. “PERSONAJES” DEL REGLAMENTO

NEOLEGIS

RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

- Ampliación regulación ET inspirada por la normativa española:
  - RT debe recurrir a ET que ofrezca suficientes garantías de cumplimiento: Códigos conducta, Certificación.
  - Contrato obligatorio, contenido obligatorio. Posibilidad uso cláusulas contractuales tipo.
  - ET seguirá instrucciones RT salvo obligación legal. Informará si las instrucciones incumplen RGPD u otras normas PD.
  - Regulación subcontratación: responsabil. ET principal.
  - Devolución o destrucción datos al finalizar sv.
  - Si un ET determina fines y medios tto se considerará RT
- Introducción regulación CORRESPONSABILIDAD: Determinación responsabilidades en el cumplimiento obligaciones RGPD

DELEGADO DE PROTECCIÓN DE DATOS

- Designación obligatoria por RT y ET (posible ampliación supuestos por EM):
  - Administraciones Públicas
  - Empresas cuya actividad principal consista en el tratamiento de datos que, en virtud de su naturaleza, alcance o fines requiera el **seguimiento periódico y sistemático de las personas a gran escala**.
  - Empresas cuya actividad principal consista en el tratamiento de datos **a gran escala** de datos sensibles (salud, ideología, religión, raza, datos genéticos, biometría, vida u orientación sexual, condenas penales…)
- Empleado o externo, independiente, rendirá cuentas al más alto nivel y se le debe dotar de recursos necesarios y formación
- Designación debe realizarse en función de cualidades profesionales y conocimientos especializados y su práctica en protección de datos
- Funciones: informar, asesorar, supervisar, cooperar y ser punto de contacto con AC

ÍNDICE DE ASPECTOS A TRATAR

5. LA PRIVACIDAD DESDE EL DISEÑO Y LA PRIVACIDAD POR DEFECTO, EL REGISTRO

NEOLEGIS

Protección de datos desde el diseño y por defecto

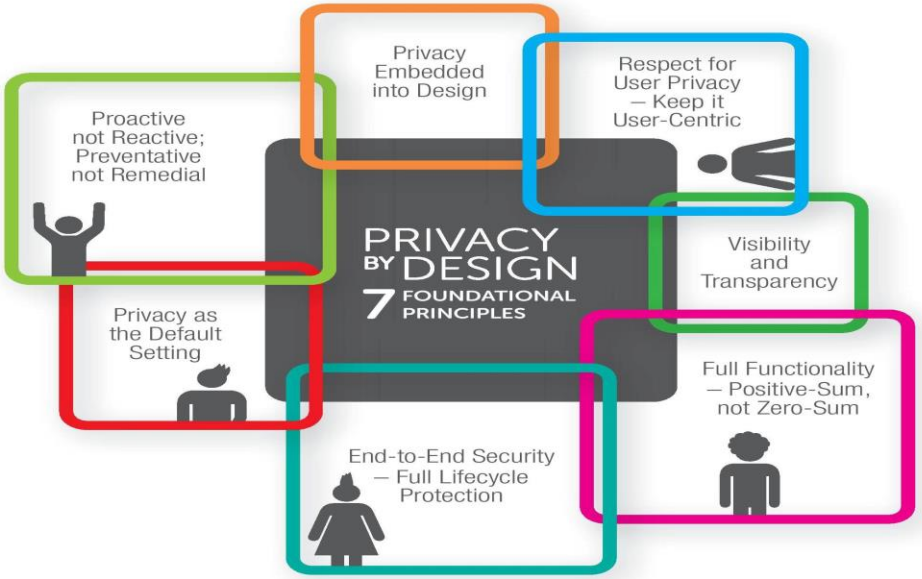
- ✓ **Protección de datos desde el diseño:** teniendo en cuenta el estado de la técnica, coste, naturaleza, ámbito contexto y fines del tratamiento, riesgos de diversa probabilidad y gravedad. Principios seudonimización, minimización, garantías, etc.

- ✓ **Protección de datos por defecto:** medidas técnicas y organizativas para garantizar por defecto sólo se traten datos necesarios para cada uno de los fines específicos. Cantidad, extensión, conservación, accesibilidad.

- ✓ **Certificación**

Privacy by Design

The importance of a lifecycle approach involving people and programs



BUILD PRIVACY INTO YOUR
POLICIES, PROGRAMS AND PRACTICES

State Government Victoria

Commissioner for Privacy and Data Protection

Representantes de responsables o encargados de tratamiento no establecidos en la Unión

- El Reglamento se aplica a tratamiento de datos de interesados que residan en la UE por responsable o encargado **no establecido** en la Unión (tratamiento relacionado con oferta de bienes o servicios, control de comportamiento en la UE).
- Designación por escrito de un **representante** en la Unión.

- Excepciones: tratamiento ocasional, no manejo a gran escala categorías especiales, datos penales, autoridades u organismos públicos.

Registro de las actividades de tratamiento

- Cada responsable, y en su caso, su representante, llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.

- Nombre, datos de contacto, fines del tratamiento, categorías de interesados, categorías datos personales, destinarios, transferencias, plazos.
- La misma obligación para el encargado de tratamiento.
- **Excepción:** menos 250 empleados, o aún así haya riesgos derechos y libertades, datos especiales.

ÍNDICE DE ASPECTOS A TRATAR

6. SEGURIDAD DEL TRATAMIENTO, NOTIFICACIONES Y EVALUACIONES DE IMPACTO

NEOLEGIS

Seguridad del tratamiento

- A) La seudonimización y el cifrado de datos personales
- B) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resilencia
- C) Disponibilidad en caso incidente
- D) Proceso de verificación, evaluación y valoración

Seguridad del tratamiento

- E) Enfoque a riesgos
- F) Adhesión a un código de conducta o un mecanismo de certificación

Notificación de una violación de la seguridad de los datos a la autoridad de control

- Violación de seguridad
- Plazo de 72 horas notificará a autoridad competente

- **Excepción:** que sea improbable que dicha violación de la seguridad constituya un riesgo para derechos y las libertades de las personas físicas

Comunicación de una violación de los datos personales del interesado

- Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

Evaluación de impacto relativa a la protección de datos

- Tratamiento que entrañe alto riesgo para los derechos y libertades de las personas físicas
- Asesoramiento del DPO
- En particular se requerirá:
- Perfiles, datos especiales, observación sistemática a gran escala de una zona de acceso público
- Lista de operaciones de tratamiento publicados por la autoridad de control

Consulta previa

- El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección datos muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo

- Asesoramiento por escrito al responsable en ocho semanas (prorrogables a 6 semanas)

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

apdcat
Autoritat Catalana de Protecció de Dades

ÍNDICE DE ASPECTOS A TRATAR

7. CÓDIGOS DE CONDUCTA Y CERTIFICACIONES

NEOLEGIS

Códigos de conducta

- Códigos destinados al cumplimiento del Reglamento
- Pueden ser sectoriales
- Las asociaciones y organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar dichos códigos

Certificación

- Mecanismo de certificación en materia de protección de datos
- Sellos y marcas de protección de datos a fin de demostrar el cumplimiento
- Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas
- Autoridades de control y organismos de certificación

RETOS Y OPORTUNIDADES

RETOS

- Hay que pensar en clave europea y empezar de nuevo. **Página en blanco.**
- Norma que introduce **elementos de valoración**
- Requerirá de **capacitación para afrontar nuevos enfoques** que exigirá perfiles multidisciplinares (jurídico, técnico, gestión).

OPORTUNIDADES

- Una norma que exigirá una adaptación por parte de todas las organizaciones, públicas y privadas: **necesidad de asesoramiento** global pero también local
- Algunas obligaciones inspiradas en la legislación española. **Somos referente.**
- Demanda de **profesionales con las capacitaciones del nuevo enfoque (DPO). Filosofía ISACA.**

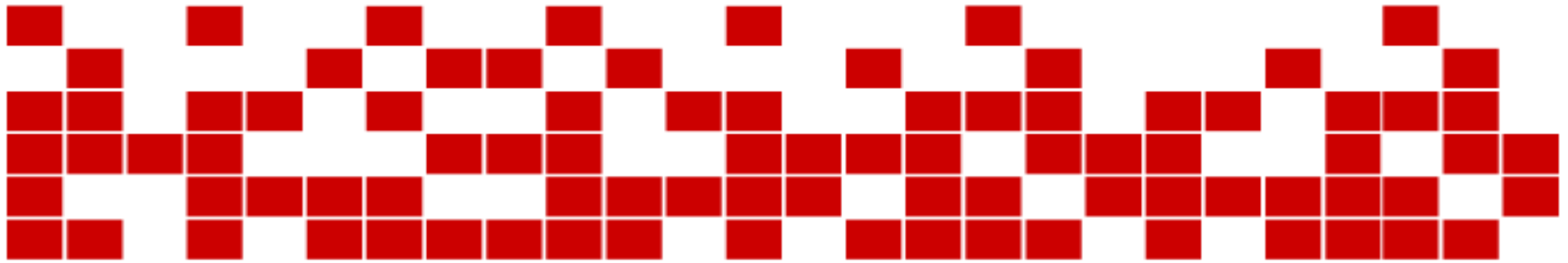
ISACA®
Trust in, and value from, information systems
Barcelona Chapter

NEOLEGIS

Belén Durán

bduran@neolegis.com

@BelenDuranCardo



ISACA®
Trust in, and value from, information systems
Barcelona Chapter

Josep Cañabate

josep.canabate@uab.cat

@josep_canabate