UNIVERSITÀ DI TRENTO

DIPARTIMENTO
FACOLTÀ DI GIURISPRUDENZA

lawtech
The Law and Technology Research Group

Confindustria Trento - Cybersecurity Talks

Privacy by design e obblighi di sicurezza: approcci innovativi per la protezione dei dati personali

21 marzo 2023

Giorgia Bincoletto

Ph.D., Assegnista di ricerca presso la Facoltà di Giurisprudenza dell'Università di Trento

Agenda

1. La protezione dei dati personali e la disciplina della cybersecurity «in pillole»
2. Accountability, obblighi di sicurezza e privacy by design
3. Considerazioni conclusive

1. La normativa sui dati personali

1. General Data Protection Regulation (GDPR) - Regolamento 2016/679

2. Codice in materia di protezione di dati personali ("Codice Privacy") – D.lgs. 196/2003

1. Alcuni concetti chiave

Dato personale

Trattamento dei dati (attività dalla raccolta alla cancellazione)

Ruoli

1. Ruoli

Interessato al trattamento

Titolare del trattamento

Preposto al trattamento

Responsabile del trattamento, sub-responsabile e incaricato

Data Protection Officer o “responsabile della protezione dei dati”

1. Alcuni concetti chiave

Base giuridica del trattamento (es. consenso, obbligo giuridico)

Finalità del trattamento

Informativa

Diritti dell'interessato

1. Principi

- Limitazione della finalità
- Minimizzazione
- Riservatezza
- **Accountability (responsabilizzazione) e privacy by design**
- **Sicurezza dei dati** (integrità e confidenzialità)

1. Cybersicurezza

“insieme di tecnologie, programmi, processi e tecniche concepiti e messi in atto per proteggere dispositivi, **dati** e reti informatiche”

(Cataldo, Mula, “Cybersecurity Law”, Pacini Giuridica, 2020)

1. Disciplina della cybersicurezza

Regolamento EIDAS 2014/910 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno

Direttiva NIS 2016/1148 e D.lgs. 65/2018: sicurezza di rete e dei sistemi informativi per gli operatori dei servizi essenziali e fornitori di servizi digitali

1. Incidente e rischio

- "**rischio**" come ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi informativi

- Obbligo di notifica degli incidenti per gli operatori di servizi essenziali

1. ENISA

Agenzia Europea di sicurezza delle reti e dell'informazione (ENISA)

Regolamento 2019/881 - Cybersecurity Act

- Cybersecurity Market Analysis Framework del 14 marzo 2023
- Report su specifici settori
- Certificazione

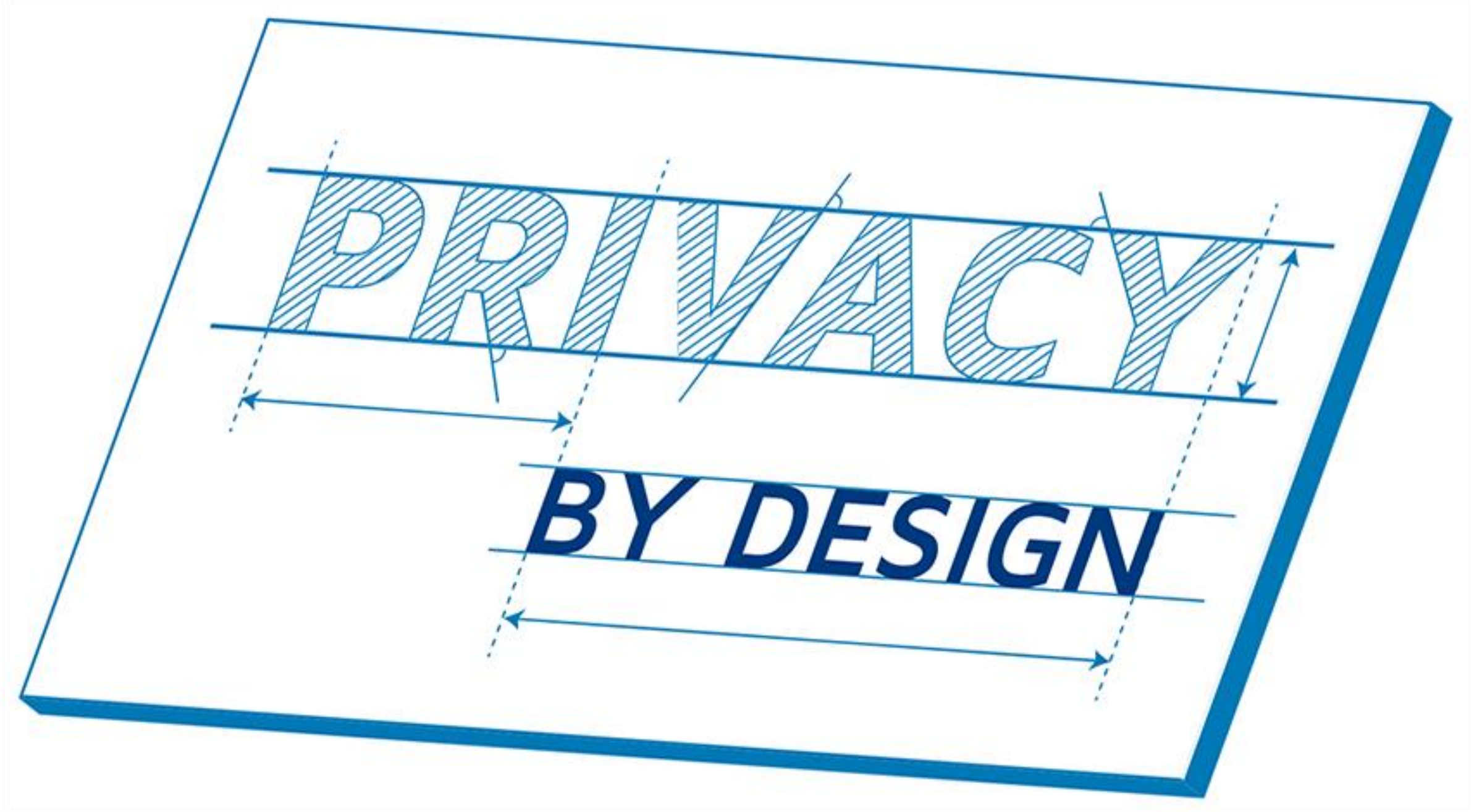

1
Malware
2
WWW
Web-based attacks
3
Phishing
4
Web application attacks
5
Spam
TOP 15 CYBER THREATS
enisa
6
DDoS
7
Identity theft
8
Data breach
9
Insider threat
10
Botnets
11
Physical manipulation, damage, theft and loss
12
Information leakage
13
Ransomware
14
Cyberespionage
15
Cryptojacking

2. Accountability, obblighi di sicurezza e privacy by design

RESPONSABILITÀ

RESPONSABILIZZAZIONE

DIMOSTRAZIONE DELLA COMPLIANCE


PRIVACY
BY DESIGN

2. Privacy by design

- Mappatura del trattamento dei dati: approccio proattivo
- Scelta di misure tecniche e organizzative (art. 25 GDPR)
- Metodo verso l'efficienza e l'adeguatezza delle soluzioni
- Monitoraggio ed aggiornamento

2. Privacy by design

2. Privacy by design

PRIMA

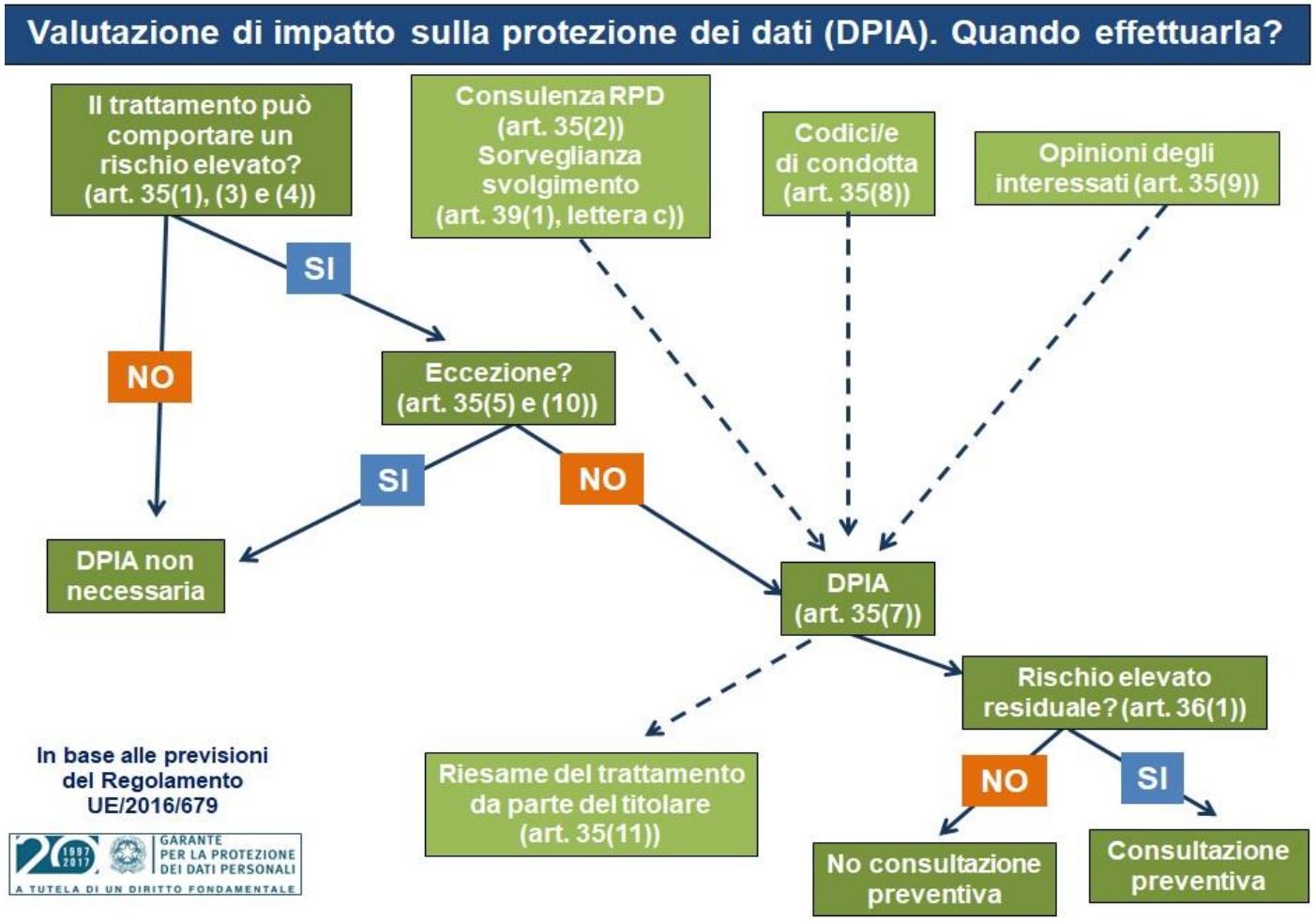
DURANTE

DOPO

2. Privacy by design

- qual è la fonte dei dati?
- chi ha raccolto i dati?
- chi sta utilizzando e dovrà utilizzare i dati?
- per quali finalità sono stati raccolti i dati?
- per quali finalità saranno conservati i dati? A chi verranno comunicati?
- i dati sono qualificabili come dati personali? Rientrano in categorie particolari di dati?
- se sono presenti dati personali, si dispone di tecniche di anonimizzazione adeguate a renderli de-identificati in modo irreversibile?

2. Valutazione di impatto



2. Privacy by design

1. Data at rest

2. Data in use

3. Data in transit

ANALISI DEL RISCHIO

2. Privacy by design

- Quali meccanismi di accesso e autenticazione sono stati previsti?
- Quale meccanismo di conservazione è stato previsto?
- I dati sono caricati nella rete Internet?
- I sistemi di conservazione sono interconnessi con altri sistemi (interni o esterni)?

2. Privacy by design

- Chi può accedere ai dati?
- Chi è coinvolto nel trattamento dei dati?
- Il settore in cui si opera è frequentemente soggetto ad attacchi di sicurezza? È mai capitato internamente?

2. Regole in materia di sicurezza

Tenere segreti i dati a terzi non autorizzati (in ogni stato)

Comunicare i dati soltanto nelle modalità corrette ed autorizzate (in transit)

Rendere accessibili i dati per finalità specifiche, ma gli accessi devono essere registrati (in use)

2. Misure di sicurezza (Art. 32 GDPR)

pseudonimizzazione e **cifratura** dei dati personali

Tecniche per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento

Tecniche per ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico

procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

2. Misure organizzative

- Predisposizione documentale (contratti, deleghe, informative e policy)
- Registro del trattamento e Valutazione di impatto
- Autorizzazioni e istruzioni interne
- Formazione in materia di privacy
- Gestione di data breach e di istanze degli interessati
- Acquisto di certificazioni o adozione di codici di condotta
- Scelta di responsabili del trattamento affidabili e di un DPO

2. Misure tecniche

- Fisiche (es., serrature, videosorveglianza, antifurto, controllo accessi)
- Informatiche (es., antivirus, firewall, VPN, criptazione, pseudonimizzazione)

→ No “one size-fits-all”, ma guardare al contesto concreto del trattamento dei dati

2. In caso di data breach

- **notificare** l'accaduto al **Garante** senza ingiustificato ritardo e, ove possible, **entro 72 ore**
  - a meno che sia improbabile che la violazione presenti un rischio

- **notificare** l'accaduto **all'interessato** senza ingiustificato ritardo, se la violazione presenta un rischio elevato per i suoi diritti

3. Considerazioni conclusive

- Certificazioni e codici di condotta
- Supporto del DPO
- Sviluppo dei processi con approccio di privacy by design → visione proattiva

Giorgia Bincoletto

E-mail:
giorgia.bincoletto@unitn.it

Web:
https://webapps.unitn.it/du/it/Persona/PER0123289/
http://lawtech.jus.unitn.it/

Copyright