OVERVIEW DEL GDPR: I CONCETTI CHIAVE

Marco Pozzoni

21 novembre 2017

MARCO POZZONI

- Associate Partner P4I – Partners4Innovation
- Heah of ICT Governance – Partners4Innovation
- Senior Advisor Osservatori Digital Innovation del Politecnico di Milano

NOVITÀ DEL REGOLAMENTO

- Registro dei trattamenti
- Accountability del titolare
- Entità delle sanzioni
- Nuovi diritti degli interessati: portabilità, oblio, conservazione, …
- Responsabilità solidale di titolare e responsabile
- Sicurezza basata su analisi dei rischi e adozione di misure tecniche e organizzative adeguate
- Obbligo di notifica dei Data breach
- Data protection by design e by default
- Valutazione d'impatto e consultazione preventiva
- Data Protection Officer (DPO)
- Certificazione dei trattamenti

REGISTRO DEI TRATTAMENTI COME ASSET

- Impostare un modello che possa garantire la **dimostrabilità degli adempimenti** previsti dalla normativa e l'allineamento con i principali «oggetti» aziendali

Processo / macro-attività

Trattamento e finalità del trattamento

Base giuridica e modalità di raccolta consenso

Categorie di dati trattati e di interessati

Termini di conservazione dei dati

Referente interno e categorie di soggetti autorizzati

Responsabili del trattamento (esterni)

Categoria destinatari dei dati

Trasferimento dati personali all'estero

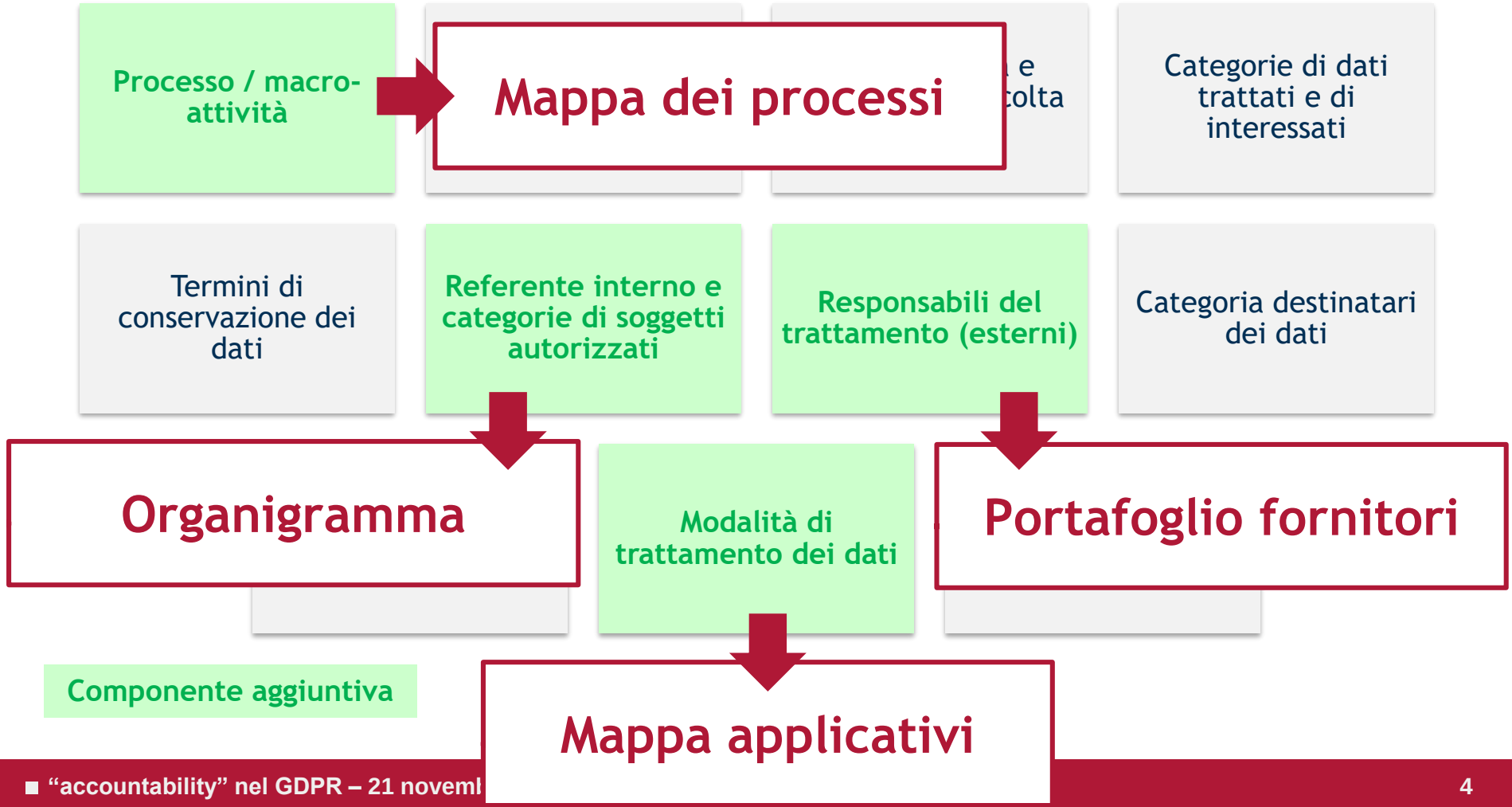
Modalità di trattamento dei dati

Misure di sicurezza tecnico-organizzative

Componente aggiuntiva

REGISTRO DEI TRATTAMENTI COME ASSET

- Impostare un modello che possa garantire la **dimostrabilità degli adempimenti** previsti dalla normativa e l'allineamento con i principali «oggetti» aziendali



ACCOUNTABILITY: UN CAMBIO CULTURALE

- Con il Regolamento UE 2016/679 definito il Legislatore europeo ha rovesciato la prospettiva della disciplina di riferimento concependo un quadro normativo tutto incentrato **sui doveri e la responsabilizzazione del titolare del trattamento ("accountability")**

- Il testo del RGPD si sviluppa essenzialmente **su processi, attività, misure tecniche e organizzative, sanzioni e obblighi rivolti a titolare (e responsabile) del trattamento**, mentre la Direttiva 95/46 era prevalentemente incentrata sui diritti dell'interessato

CONCETTO DI ACCOUNTABILITY

Liceità, correttezza e trasparenza

trattati in modo lecito, corretto e trasparente nei confronti dell'interessato

Limitazione della finalità

raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità

Minimizzazione dei dati

adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati

Esattezza

esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati

Limitazione della conservazione

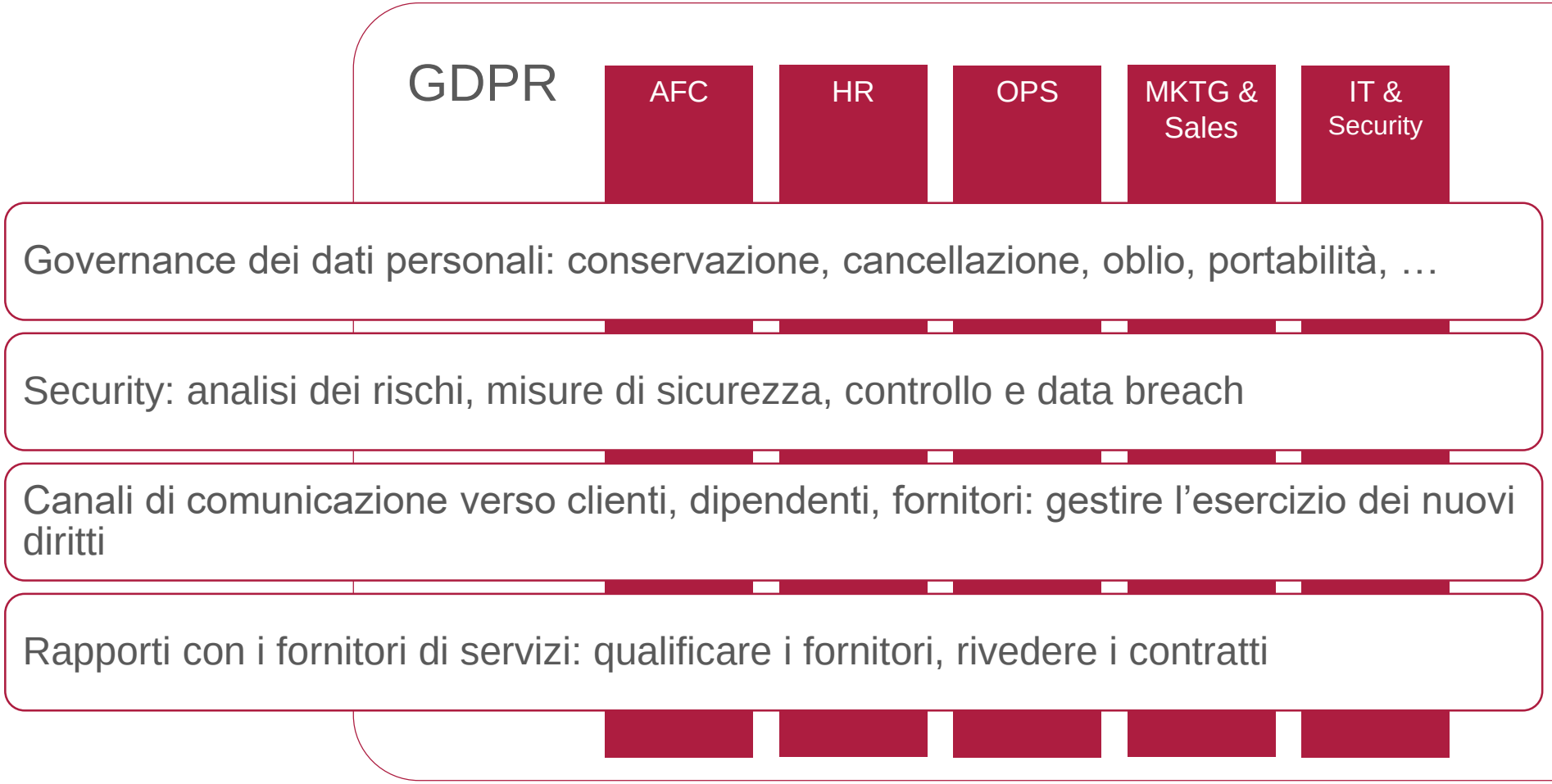
conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati

Integrità e riservatezza

trattati in maniera da garantire un'adeguata sicurezza dei dati personali

Il titolare del trattamento è competente per il rispetto dei suddetti principi e in grado di comprovarlo («responsabilizzazione»)

PRINCIPALI IMPATTI DEL GDPR SULL'IT



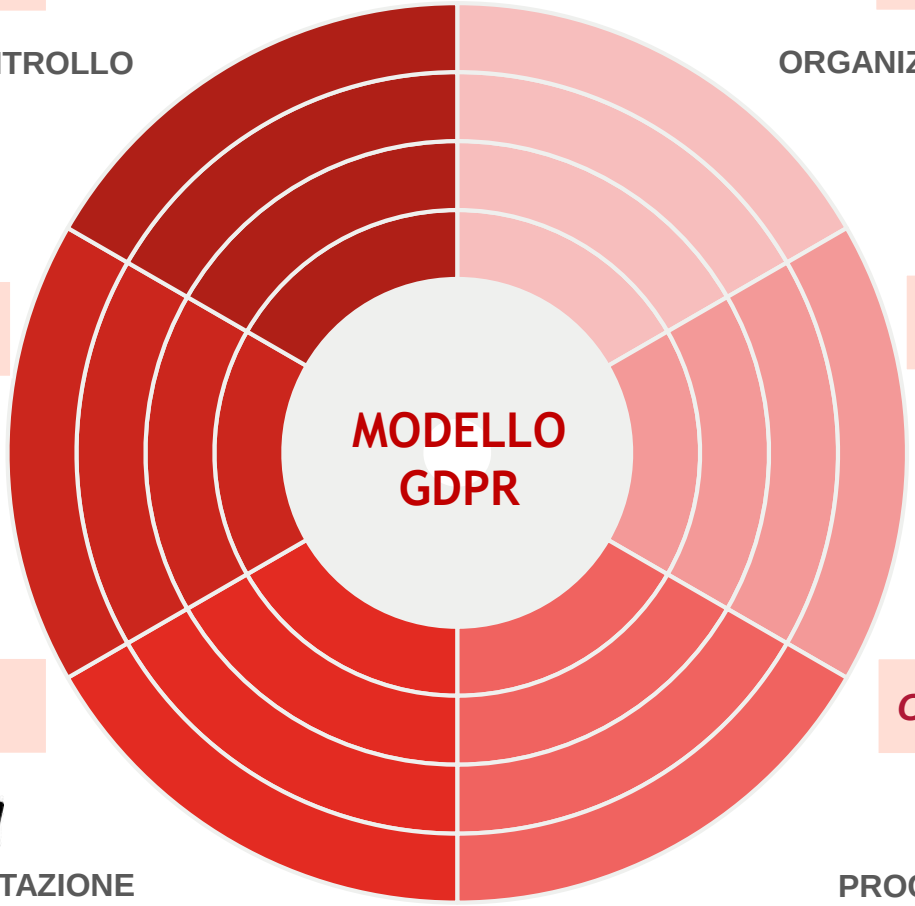
GESTIONE DEL GDPR

Audit

SISTEMA DI CONTROLLO

Organization; Audit

ORGANIZZAZIONE E RUOLI



Information Technology

TECNOLOGIA E
STRUMENTI

Human Resources

PERSONE, CULTURA
E COMPETENZE

Legal; Compliance

DOCUMENTAZIONE

Organization; Compliance

PROCESSI E REGOLE

SANZIONI AMMINISTRATIVE GARANTE 2013-2015

Fino a oggi le sanzioni sono state tendenzialmente contenute

SANZIONI AMMINISTRATIVE GDPR (ART. 83)

Il Regolamento prevede la possibilità per le Autorità nazionali di **sanzionare fino a € 20.000.000** o, in caso di «undertaking», **al 4% del fatturato globale annuo**, a seconda di quale risulti la sanzione più elevata

Sanzioni più alte:

- violazioni dei principi del trattamento, incluse le condizioni per il consenso
- violazione dei diritti degli interessati
- inosservanza delle norme in tema di trasferimento internazionale dei dati

Sanzioni più basse (fino a €. 10.000.000 o al 2% del fatturato globale annuo) si applicano, fra l'altro, a:

- violazione delle obbligazioni di titolare e responsabile del trattamento, incluso gli obblighi di sicurezza e data breach notification

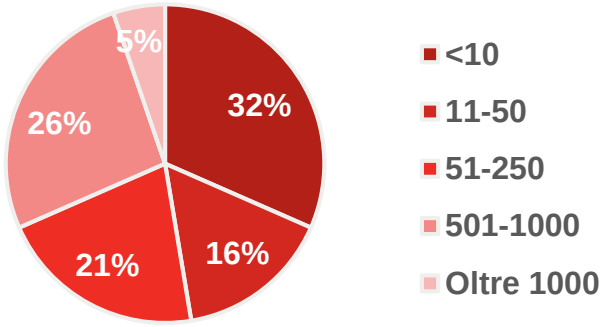
- Il concetto di ***'undertaking***' potrebbe mettere a rischio le *revenues* di un gruppo societario, anche se non tutte le società del gruppo sono responsabili della violazione.
- La sanzioni non sono infatti imposte in riferimento alle revenues della specifica società sanzionata, ma alle revenue di un "undertaking". Ciò, in estrema sintesi, potrebbe comportare che, se la società sanzionata è parte di un "undertaking", il 4% o 2% saranno calcolati sul fatturato totale annuo dell'intera undertaking e non il fatturato totale annuo della sola specifica società sanzionata.

IL GDPR IN AZIENDA

I RISULTATI DELLA SURVEY

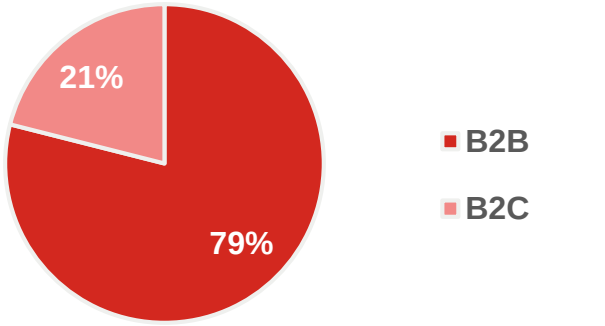
IDENTIKIT DEI RISPONDENTI

Dimensione



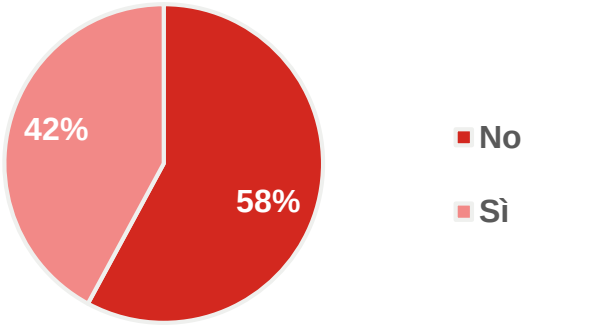
Buon mix dimensionale a rappresentanza di grandi, medie e piccole aziende

Attività svolte



Preponderanza di aziende B2B, che comporta tipicamente un numero minore di trattamenti

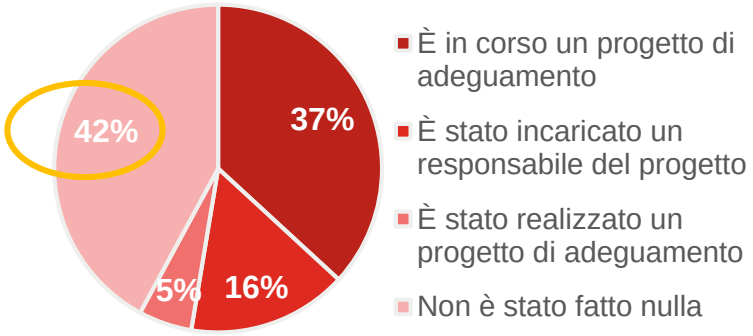
Fornisce servizi che comportano trattamento di dati personali
(es. call center, outsourcing)



Buona rappresentanza di aziende che forniscono servizi che comportano trattamento di dati personali

LIVELLO DI RECEPIMENTO

Recepimento GDPR

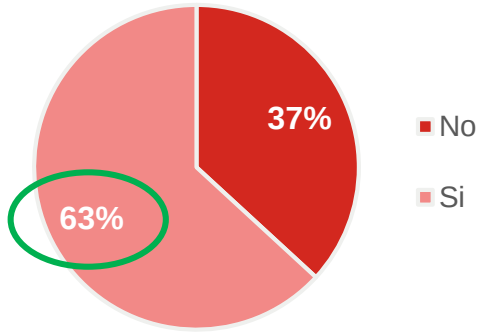


Fa riflettere il 42% di aziende che non è ancora partita con un progetto di adeguamento

Budget per gli adeguamenti

Molti degli interventi tecnologici, ma anche organizzativi, necessiteranno di risorse

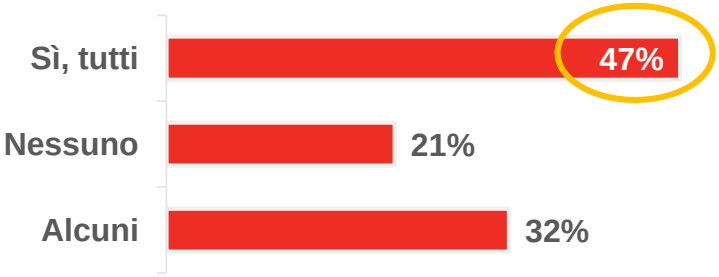
Misure di sicurezza a seguito di analisi dei rischi



Molte aziende hanno probabilmente continuato ad aggiornare il DPS, nonostante la non obbligatorietà

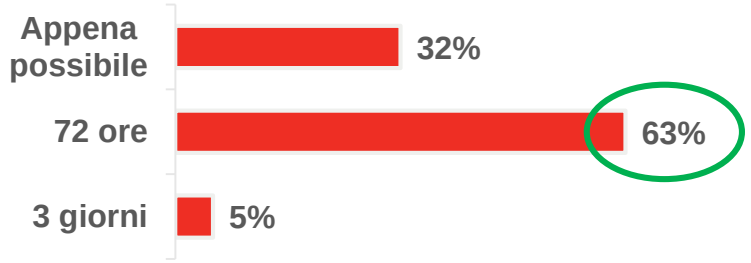
LIVELLO DI CONOSCENZA

Saprebbe definire i seguenti termini: Co-titolare, Responsabile, Categorie particolari di dati personali, Trattamento, Accountability?



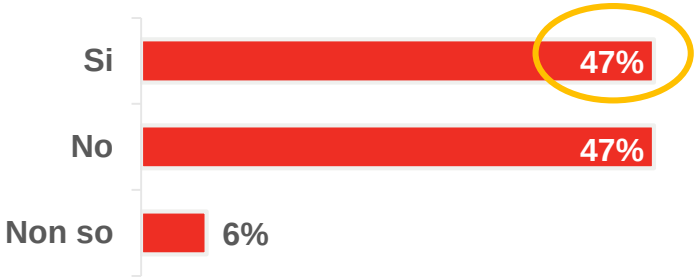
Definizioni

Entro quanto tempo deve essere effettuata la notifica al Garante delle violazioni di sicurezza che possono comportare rischi per gli interessati?



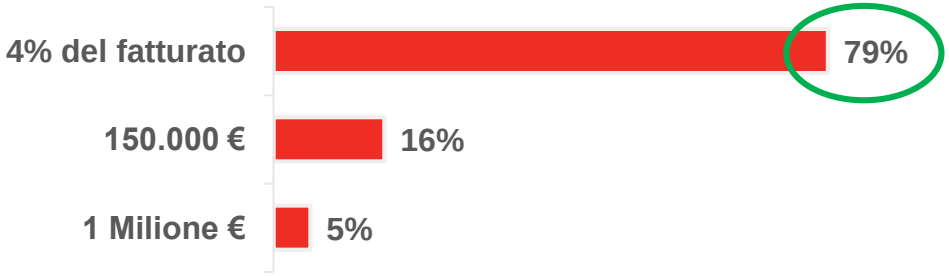
Data Breach

By Design



Il GDPR introduce il concetto di Data Protection by Design. È un tema conosciuto in azienda?

Sanzioni



Le sanzioni previste in caso di inadempienza possono arrivare fino a quale valore?