bmisystem®

Governare il RGPD:
gestire gli adempimenti Privacy nel continuo

TRANSPARENCY | COMPLIANCE | ANTI-CORRUPTION | DATA PRIVACY

Février 2018

Agenda

- RGPD: Aumentare il valore dell'azienda

  Jérôme Martinez CEO BMI SYSTEM

- La data governance nel RGPD

  Avv. Maria Roberta Perugini – Jacobacci & Associati

- ORYGA: un approccio dotato di una gestione continua della conformità

  Jérôme Martinez CEO BMI SYSTEM

- Dibattito

RGPD: Aumentare il valore dell'azienda

Jérôme Martinez

1

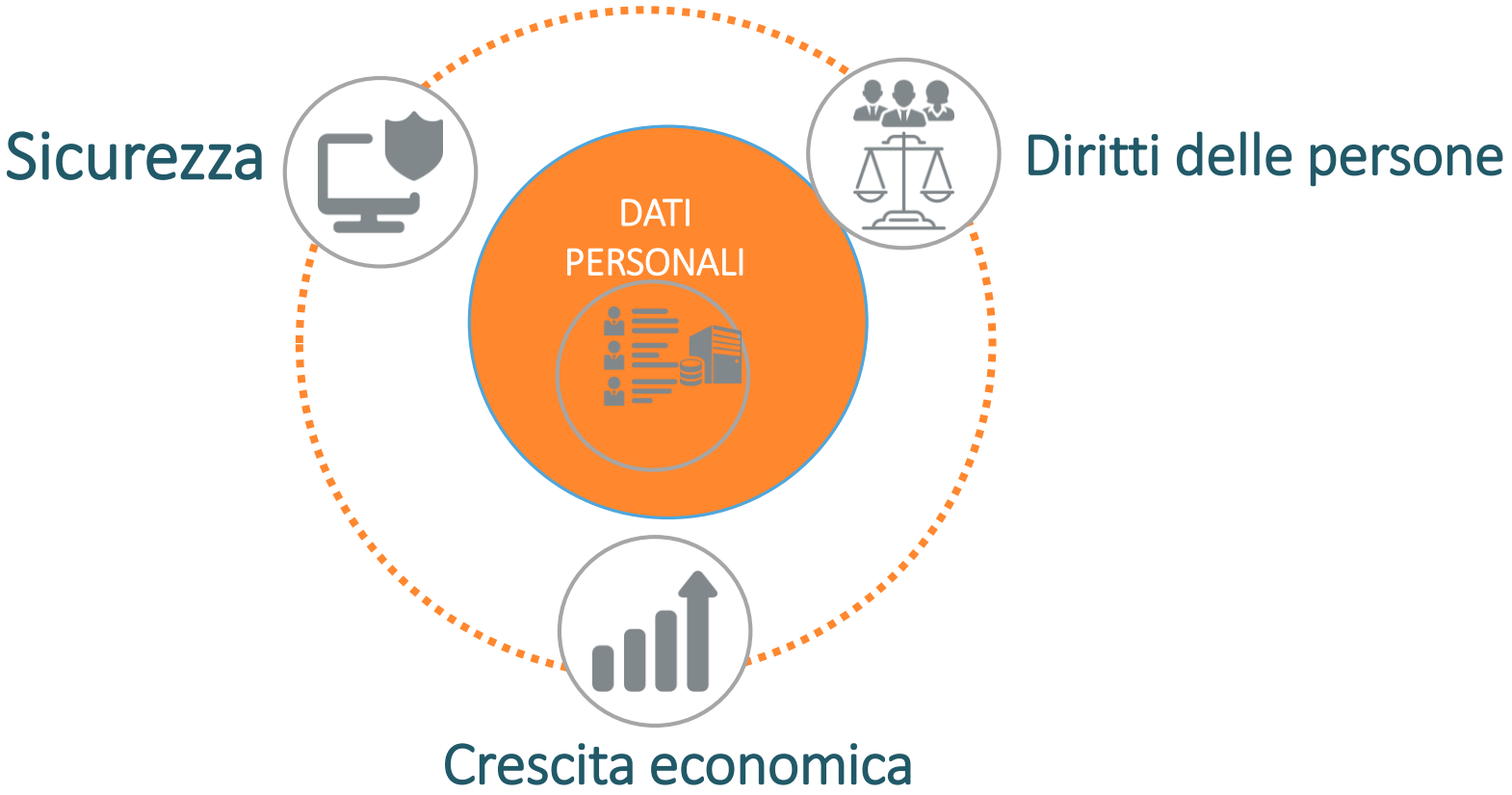
BMI SYSTEM, Leader francese nelle soluzioni di gestione della conformità l Trasparenza

- Fondata nel 2004, con sede a Parigi (Montrouge)
- L' unico editore francese di software dedicato alla conformità e trasparenza per l'industria farmaceutica e dei dispositivi medici.
- ISO 9001 e presto certificazione ISO 27001

Un know-how sviluppato su una solida base di clienti molto esigenti

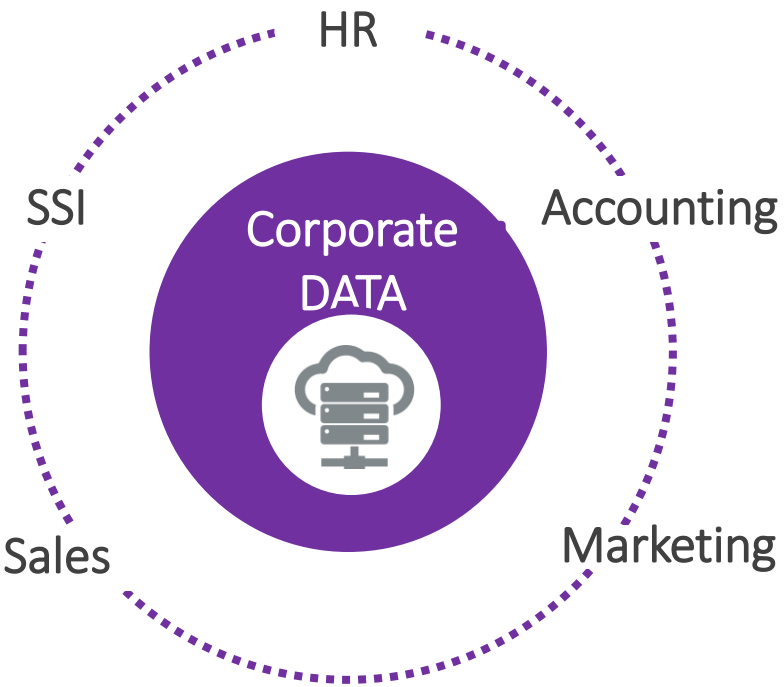
- Forte copertura clienti: +40 clienti in oltre 50 paesi
- +50 dipendenti
- Competenza e know-how tecnologico, commerciale e regolamentare
- Crittografia del percorso di controllo e competenza Privacy by Design

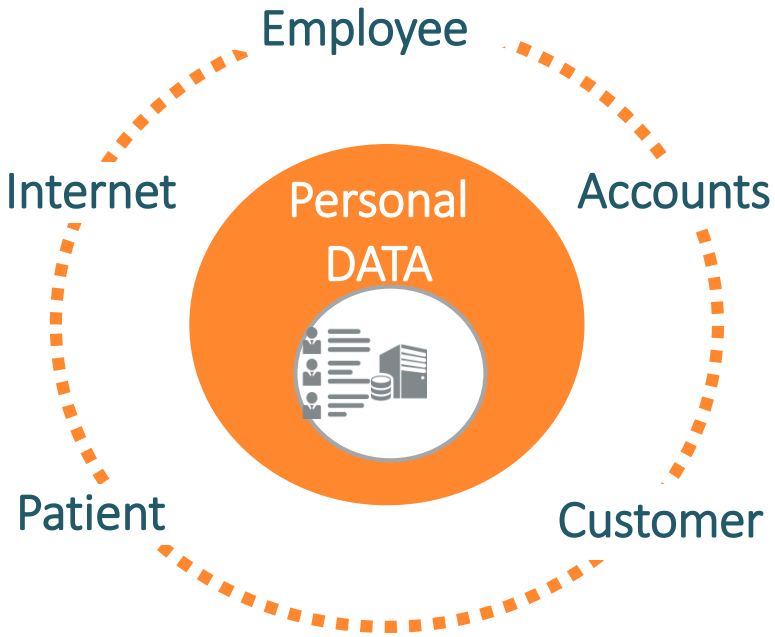
RGPD/GDPR: circolazione e scambio di dati personali



Governance dei dati personali

Nuovi diritti => cambiamento di paradigma





Rischi e sanzioni

2 Tipi di RISCHI

Rischi finanziari

- Sanzioni amministrative
  -Max. 20M€ o 4% GCAG-
- Cause civili
- Class action

Rischi operativi

- Immagine & Reputazione
- Revoche del Consenso di massa
- Bloco del trattamento
- Cancellazione dei dati personali

La data governance nel RGPD

Avv. Maria Roberta Perugini

2

Financial Conduct Authority

Feedback Statement FS16/4

Call for input on supporting the development and adopters of RegTech

July 2016

Integrate, standardise and understand

Technology that drives efficiencies by closing the gap between intention and interpretation

Semantic tech and data point models
Technology that converts regulatory text into a programming language.

- Machine-readable regulation would allow more automation and could significantly reduce the cost of change.
- It could also help ensure greater consistency between the intentions of a regulation and its implementation.

Shared data ontology
A formal naming and definition of the types, properties, and interrelationshi entities.

- Sharing a common understanding of the structur regulatory data would improve efficiency, reduce ease interactions and help remove ambiguity.

Application Programme Interface (API)
Technology that allows systems to interact consistently, in this case, over the internet.

Robo-Handbook
Technology that allows firms to intera with regulation to understand the imp of this to their systems and processes.

- A more interactive FCA Handbook better tailored the firm's permissions could make compliance an reporting requirements clearer.

erability

y and provide

Efficiency and collaboration

Technology that allows more efficient methods of sharing information

Alternative reporting methods
Technology that allows data to be provided (or taken) in a different way.

- Creating more flexibility for firms to provide their regulatory data would reduce the costs and the burden of regulatory reporting.
- For example, making it easier for firms to use different software to provide data to the regulator may allow them to streamline processes and align internal systems.

Shared utilities
Technology that allows firms to share services (such as a Know Your Customer utility) via the cloud and/or online platforms.

- Shared solutions can reduce the burden and regulatory costs for the industry by increasing scalability and flexibility.

The cloud/cloud computing
On-demand computing services delivered over the Internet.

- Its flexibility allows firms to greatly improve efficiency and reduce costs.
- Access to innovative software and advanced computing allows firms to improve capabilities, deliver better insights and make better decisions.

Online platforms
Technology that helps different parties communicate.

- Greater FCA engagement would help increase the FinTech community's understanding of regulation and compliance, potentially enabling it to develop more effective RegTech.
- It would encourage FinTech to be engaged earlier in policy design.

lata, allows better decision making and the creation of

s that can
ructured and
be stored in
ories).
data sets
more informed

could also reduce
ms.

nology
simulation of
ssess their
hole.
impact (and
on to be

ms'

Risk and compliance monitoring
Technology that allows an always-on, non-invasive surveillance of transactions, behaviour and communications.

- Identifying real-time risk/fraud through correlating multiple sources of information and using powerful calculation engines could reduce risk and the number of false positives.

Machine learning and cognitive technology
Technology that learns from data and pattern recognition to refactor / change algorithms (e.g. artificial intelligence).

- As this allows systems to automatically reassess and refine processes in reaction to input from users, it could replace firms' slightly more complex high-volume and repeatable regulatory tasks.

New directions

Technology that allows regulation and compliance processes to be looked at differently (please note that this is not an exhaustive list)

Blockchain/distributed ledger
This securely records and encrypts verified data that can be safely shared across a network held in a distributed database.

- Distributed ledgers could improve system integrity and increase transparency.
- They could transform processes, reduce costs and potentially redefine how data is shared.

Inbuilt compliance
Regulatory requirements can be coded into automated rules applied when relevant.

- A system that can automatically apply the regulatory 'programme code' would improve compliance, reducing regulatory and staff costs.

Biometrics
Technology that measures and analyses people's physical and behavioural characteristics.

- Biometric technology could allow more efficient and/or robust ways to verify identity.

System monitoring and visualisation
Technology that captures and traces all messages created by systems and their interactions.

- Technology that creates a visual representation of how a firm's technology is working. It looks at the 'flow of systems' by monitoring and capturing events such as mouse clicks, key presses, or messages from other programmes. This allows firms to visualise their entire technology estate and could help inefficiencies to be identified.

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

Il GDPR

RESPONSABILITÀ ATTIVA DEL TITOLARE E DI TUTTI I SOGGETTI ATTIVI DEL TRATTAMENTO:

ACCOUNTABILITY come *compliance* dinamica, costruita «su misura», destinata a implementazione nel continuo

Obbligo di ATTUARE misure tecnologiche ed organizzative di prevenzione del rischio adeguate ed efficaci

misure CONCRETE ED EFFICACI

Per "attuare i principi di protezione dei dati" *(art. 25 – Privacy by design e by default)*

Per "garantire un livello di sicurezza adeguato al rischio" *(art. 32 - Sicurezza del trattamento)*

da individuare **autonomamente** in rapporto alle **peculiarità del caso specifico (valutazione del rischio)**

Isabelle Falque Pierrotin [*]'s speech – 16 March 2016

First: compliance obligations. The Regulation is a turning point for you, for the business: no more (or at least fewer) administrative paper work BUT more real compliance.

With the regulation, we go from static to dynamic compliance.

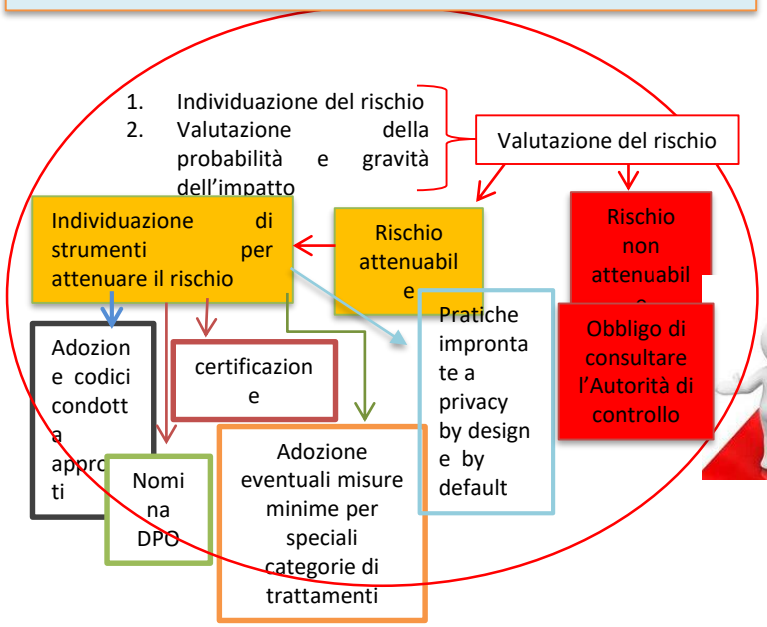
More real compliance through a wide range of tools that the company can pick and choose to ensure the best compliance possible.

[*} Presidente CNIL

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

Il GDPR

Obbligo di **ATTUARE** **misure** tecnologiche ed organizzative **adeguate ed efficaci** di prevenzione del **rischio di violazione dei diritti e libertà fondamentali degli individui**



Procedimentalizzazione della valutazione del rischio e delle azioni conseguenti

Obbligo di **DIMOSTRARE** la **conformità** del trattamento al Regolamento e **l'efficacia** delle misure

Formalizzazione delle regole e dei processi che governano le azioni di prevenzione

Art. 24 GDPR

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento («ACCOUNTABILITY»)

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

COME OPERARE PER ASSICURARE LA CONFORMITA?

ATTIVITA PREPARATORIE

- VALUTAZIONE D'IMPATTO DEL GDPR SULL'OPERATIVITA AZIENDALE
- SVILUPPO DI UN PIANO DI IMPLEMENTAZIONE
- VALUTAZIONE DELLE RISORSE DA STANZIARE

MAPPARE LO STATO DI FATTO

MISURARE LO STATO DI FATTO IN UN'OTTICA DI ACCOUNTABILITY E PRIVACY BY DESIGN E BY DEFAULT (*gap analysis*)

ESEGUIRE ANALISI DEI RISCHI E DPIA (SE NECESSARIA)

VALUTARE I COSTI DELLE MISURE

PIANIFICARE I TEMPI DI ATTUAZIONE DELLE AZIONI E GLI INVESTIMENTI

ATTRIBUIRE LE RELATIVE RESPONSABILITA

DEFINIRE GLI STRUMENTI PER DOCUMENTARE LE **AZIONI** PIANIFICATE E LE **RAGIONI** DELLA RELATIVA SCELTA

- **DEFINIRE** IL PIANO DI ATTUAZIONE
- **PREDISPORRE** IL MODELLO DI GESTIONE PRIVACY DEFINITIVO

- **CONDIVIDERE** NELL'ORGANIZZAZIONE
- **APPROVARE** LE ATTIVITA / AZIONI / MISURE INDIVIDUATE E
- **ATTUARLE**

AZIONI PER L'IMPLEMENTAZIONE:

- INTERVENTI LEGALI
- MODIFICHE ORGANIZZATIVE
- INVESTIMENTI IN TECNOLOGIA

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

CONFORMITA È: ADEGUAMENTO NEL CONTINUO

1) DEFINIRE UN PIANO DI **MANTENIMENTO E VERIFICA** PERIODICA DEI LIVELLI DI CONFORMITA INDIVIDUATI → **TEST, MONITORAGGIO DELLA LEGISLAZIONE, MONITORAGGIO DELLE MODIFICHE INTERNE AL CONTESTO AZIENDALE (trattamenti, risorse informatiche, processi aziendali) AUDIT INTERNI ED ESTERNI**

2) DEFINIRE UN PIANO PER **DIMOSTRARE** LA CONFORMITA → **REPORTISTICA**

ACCOUNTABILITY

DEFINIZIONE FORMALE DI CRITERI PER LA CONFORMITA

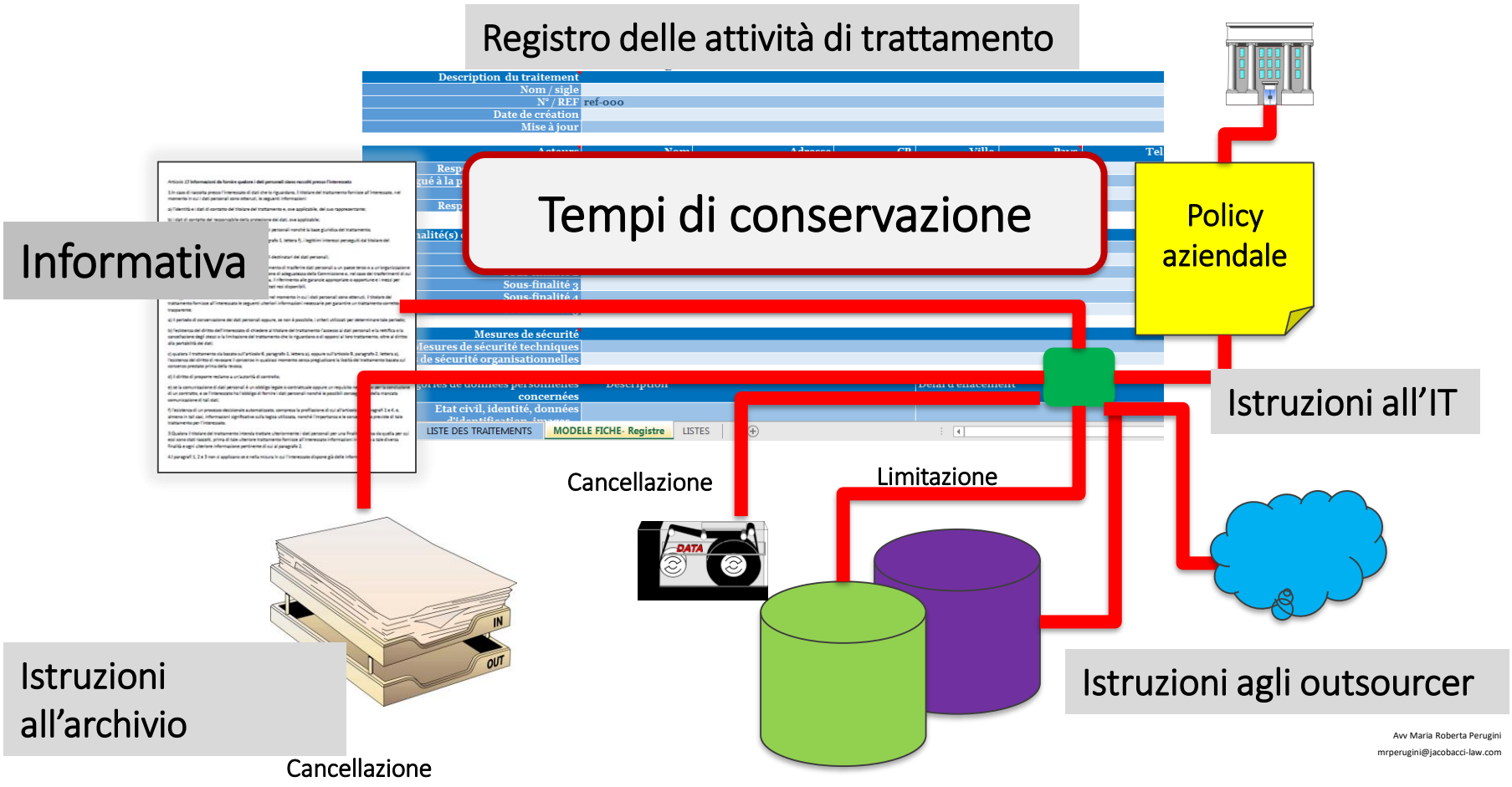
TRADUZIONE IN BEST PRACTICE E PROCEDURE DOCUMENTALMENTE FORMALIZZATE

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

LA RESPONSABILITA RISARCITORIA NEL GDPR: conseguenze pratiche

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

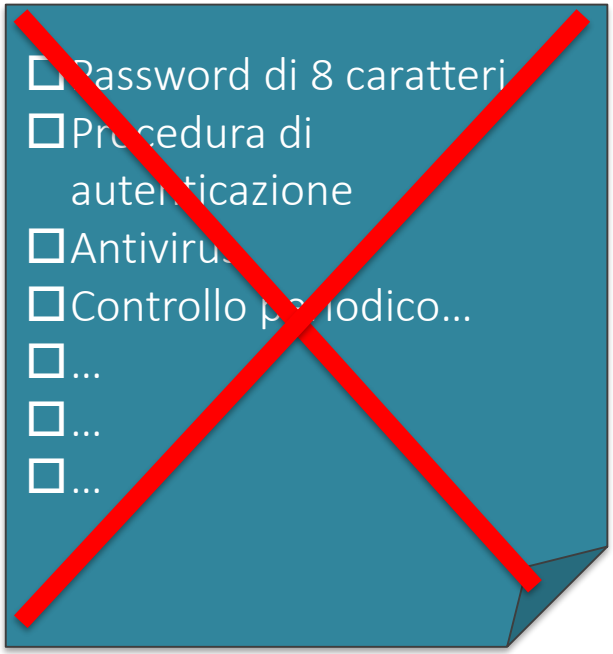
COMPLESSITÀ DEI CONTROLLI NELLE AREE FORMALIZZATE



Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

NUOVO APPROCCIO AI CONTROLLI NELLE AREE NON FORMALIZZATE

Misure di sicurezza

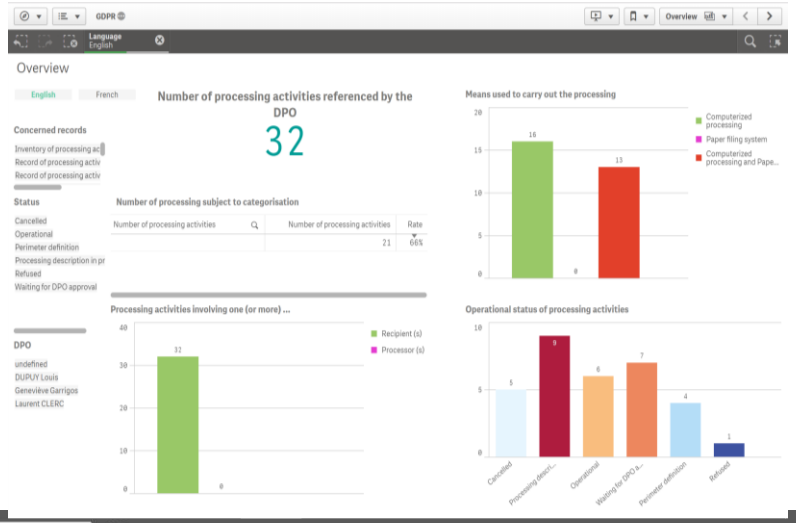


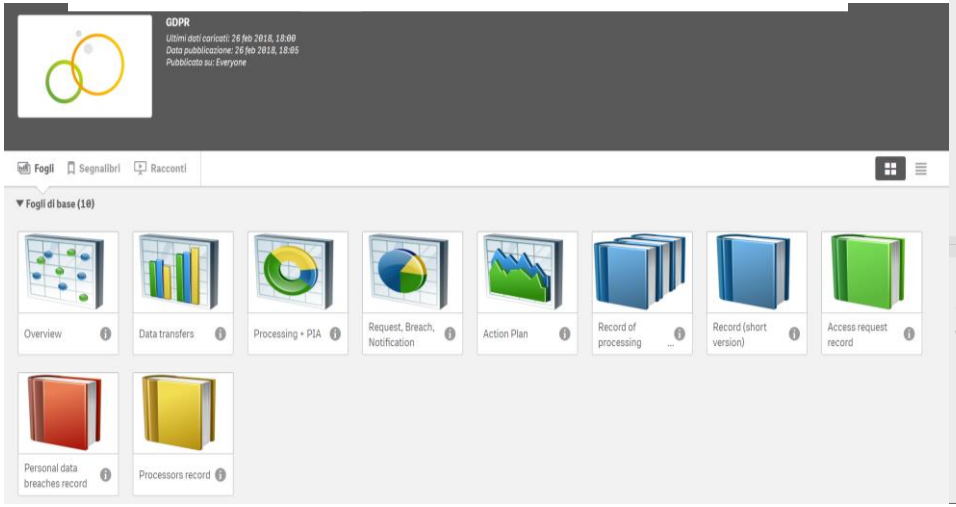
PROCESSO DECISIONALE

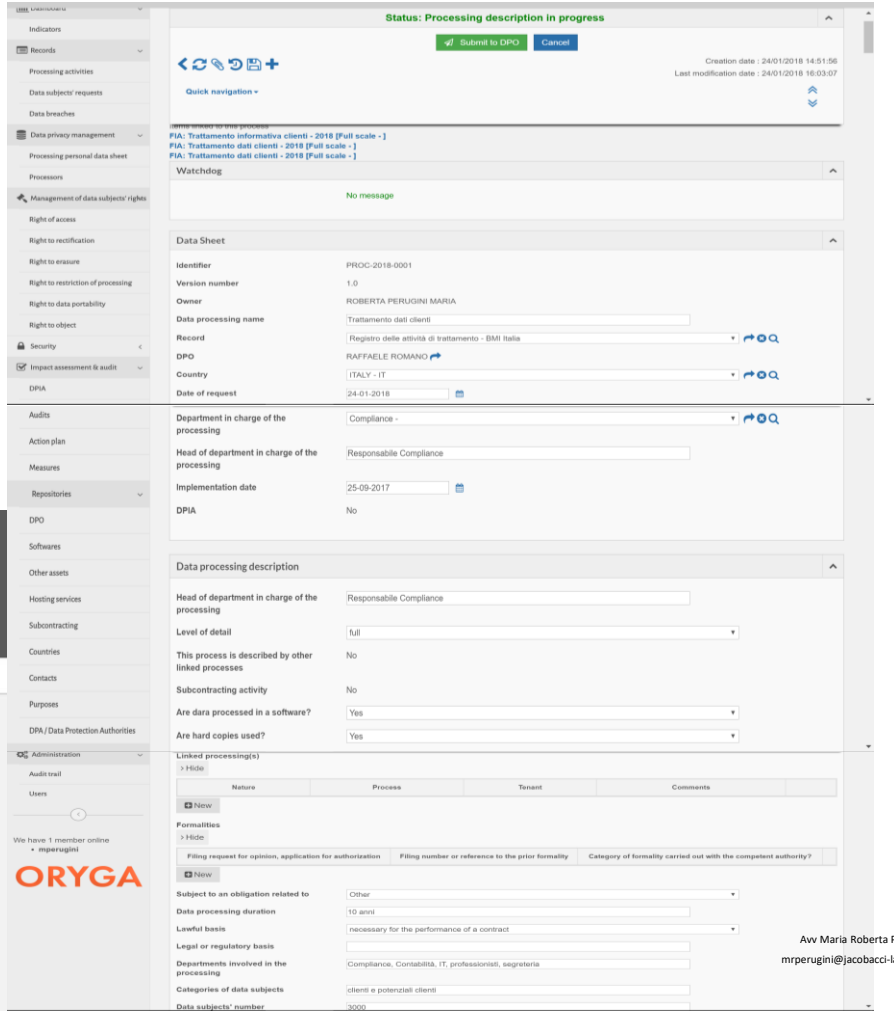
- Analisi eseguite
- Soggetti coinvolti
- …
- Assunzione di rischio
- Coinvolgimento del CdA
- Documentazione
- Designazione DPO

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

Valutazione del livello di conformità globale







Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

ORYGA : un approccio dotato di una gestione continua della conformità

Jérôme Martinez

3

ORYGA : la soluzione predisposta per il trattamento dei dati

Soluzione software SaaS per la conformità RGPD

- Piattaforma tecnologica che integra tutte le funzionalità
- Preparazione dei registri:
  - Trattamenti,
  - Appaltatori e subappaltatori,
  - Richieste di esercizio dei diritti,
  - Notifica delle violazioni di sicurezza
- Analisi d' impatto e audit, indicatori e cruscotti
- Multisito intra ed extraeuropeo, multilingue

- Gesticce i processi per la conformità RGPD
- Consente la gestione dinamica dei trattamenti dei dati personali
- Documenta tutte le operazioni e i processi che dimostrano la conformità

Mappatura del trattamento

Registri trattamenti

Organizzazione dei processi

1/

- **Privacy by design: per le applicazioni e i trattamenti**
  - Minimizzazione della raccolta dei dati, conservazione, informative, raccolta del consenso, sicurezza e riservatezza dei dati...

2/

- **Sensibilizzazione dei collaboratori e organizzazione del flussi informativi**
  - Piano di formazione e istruzione per i dipendenti

3/

- **Reclami e richieste di esercizio dei diritti**
  - Definizione degli attori e delle modalità

4/

- **Anticipare le violazioni dei dati**
  - Notifica all' autorità per la protezione dei dati entro 72 ore e agli interessati il più presto possibile.

Documento

Dimostrare il rispetto del RGPD

1/

- **Documentazione sul trattamento dei dati personali**
  - I registri dei trattamenti - per titolari e responsabili
  - Valutazioni d' impatto per trattamenti ad alto rischio per i diritti, monitoraggio dei trasferimenti di dati al di fuori dell' UE.

2/

- **Informazione delle persone**
  - Informative,
  - Modelli per raccogliere il consenso,
  - Procedure per l' esercizio dei diritti.

3/

- **Contratti con ruoli e responsabilità degli stakeholder**
  - Contratti con appaltatori e subappaltatori,
  - Procedure interne per le violazioni dei dati,
  - Prova del consenso ove necessario

Gestione dei rischi/ Valutazione d'impatto

Valutazione d’impatto: non sistematica ma raccomandata

PERCHE ?

- Valutare i rischi dal punto di vista delle persone interessate
  - Trattamento privacy-friendly
  - Impatto sulla vita privata
  - Rispetto dei principi fondamentali del RGPD

QUANDO ?

- Prima della raccolta ed elaborazione dei dati,
- Qualsiasi trattamento atto a creare rischi elevati per i diritti e le libertà delle persone fisiche.

COSA ?

- Descrizione dell' operazione di trattamento e delle sue finalità,
- Valutazione della necessità e proporzionalità del trattamento,
- Valutazione dei rischi per i diritti umani e le libertà,
- Misure previste per far fronte a tali rischi e rispettare il RGPD

BMI SYSTEM

contact@bmi-system.com