SETTING THE RIGHT GDPR PRIORITIES

Alberto, Canadè | Manager

Spike Reply

MOTORE SANITÀ - SECURITY & PRIVACY DEL DATO SANITARIO

Il Trade off tra Cybersecurity Tutela e Sviluppo del mercato

19 giugno Milano

REPLY

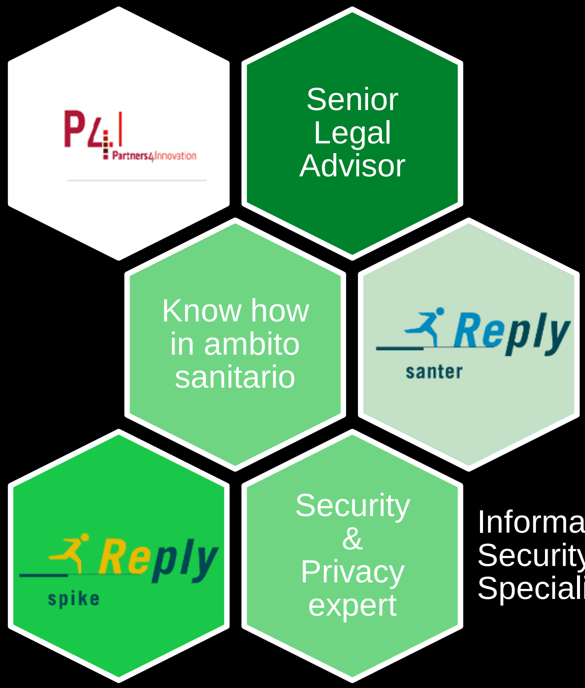
Reply è costituita da un modello a rete di aziende altamente specializzate, che affiancano i principali gruppi industriali nella definizione e nello sviluppo di modelli di business abilitati dai nuovi paradigmi tecnologici e di comunicazione, quali ad esempio, Big Data, Cloud Computing, Digital Communication, Internet degli Oggetti, Mobile e Social Networking, per ottimizzare ed integrare processi, applicazioni e dispositivi.

I servizi di **Reply** includono *Consulenza, System Integration e Digital Services*.

I **Reply** declina la propria offerta di servizi su tre ambiti di competenza: *Processi, Applicazioni e Tecnologie*.

Santer Reply è la società del Gruppo con know-how nel settore sanitario, **Spike Reply** è la società specializzata in Sicurezza delle Informazioni e Privacy.

COMPETENZE REPLY



Senior Legal Advisor

Know how in ambito sanitario

Security & Privacy expert

Information Security Technical Specialist

REPLY VALUE PROPOSITION
GOVERNANCE & COMPLIANCE

- ✓ **13 Years of experience on IT Security and Data Protection Field**: long lasting presence and strong reputation.
- ✓ **More Than 270 experts worldwide:** Italy, UK, Germany, United States and Brazil...
- ✓ **Cyber Security Command Center** with 24x7x365 operations.

- Più di 100 certificazioni
- Membro dell'"*Osservatorio Sicurezza e Privacy*" at Politecnico di Milano e "*Osservatorio Sicurezza e Frodi Informatiche*" at ABILab
- **Partnership** strategica con Gabriele Faggioli, presidente del Clusit, tramite la collaborazione con P4I, società esperta in diritto informatico

DOVE SIAMO

6K people

Americas

US
(Chicago, Detroit)
Brazil
(Belo Horizonte, Sao Paulo)

Europe

Germany
(Berlin, Bremen, Dusseldorf, Frankfurt, Gutersloh, Hamburg, Munich)
Italy
(Bari, Milano, Padova, Roma,Torino, Trieste, Verona)
The UK
(London, Basingstoke, Chester, Cockpole Green)
Benelux & France
(Amsterdam, Brussels, Luxembourg, Paris)
Poland & Romania
(Katowice, Bucharest)
Belarus
(Minsk)

Asia

China
(Beijing)

MEETING AGENDA

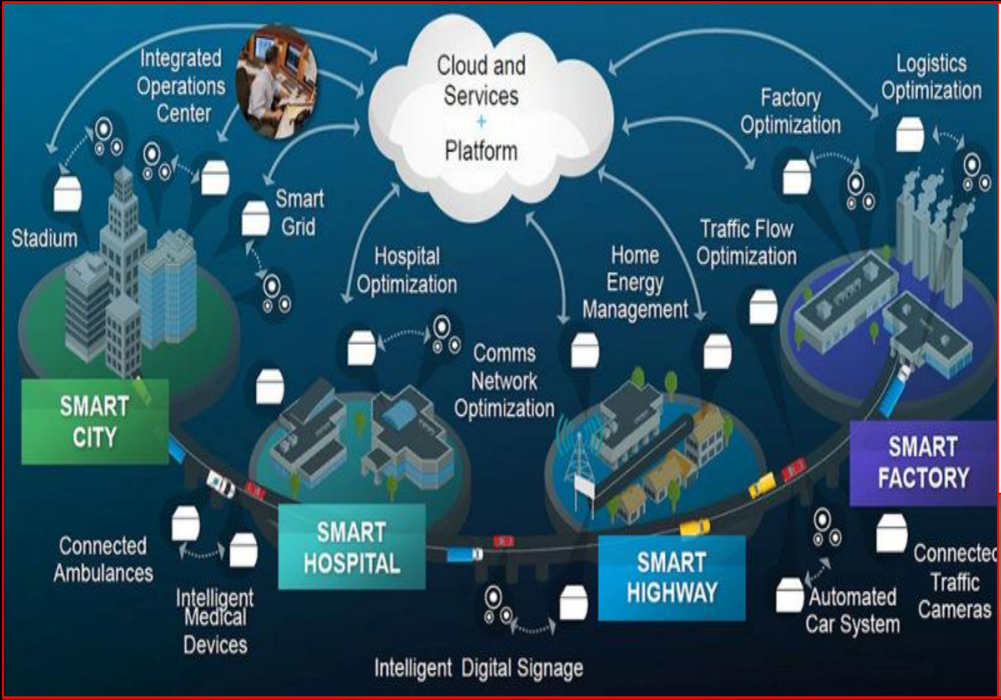
1 The context where GDPR was born

2 Setting out the right priorities for getting GDPR-ready

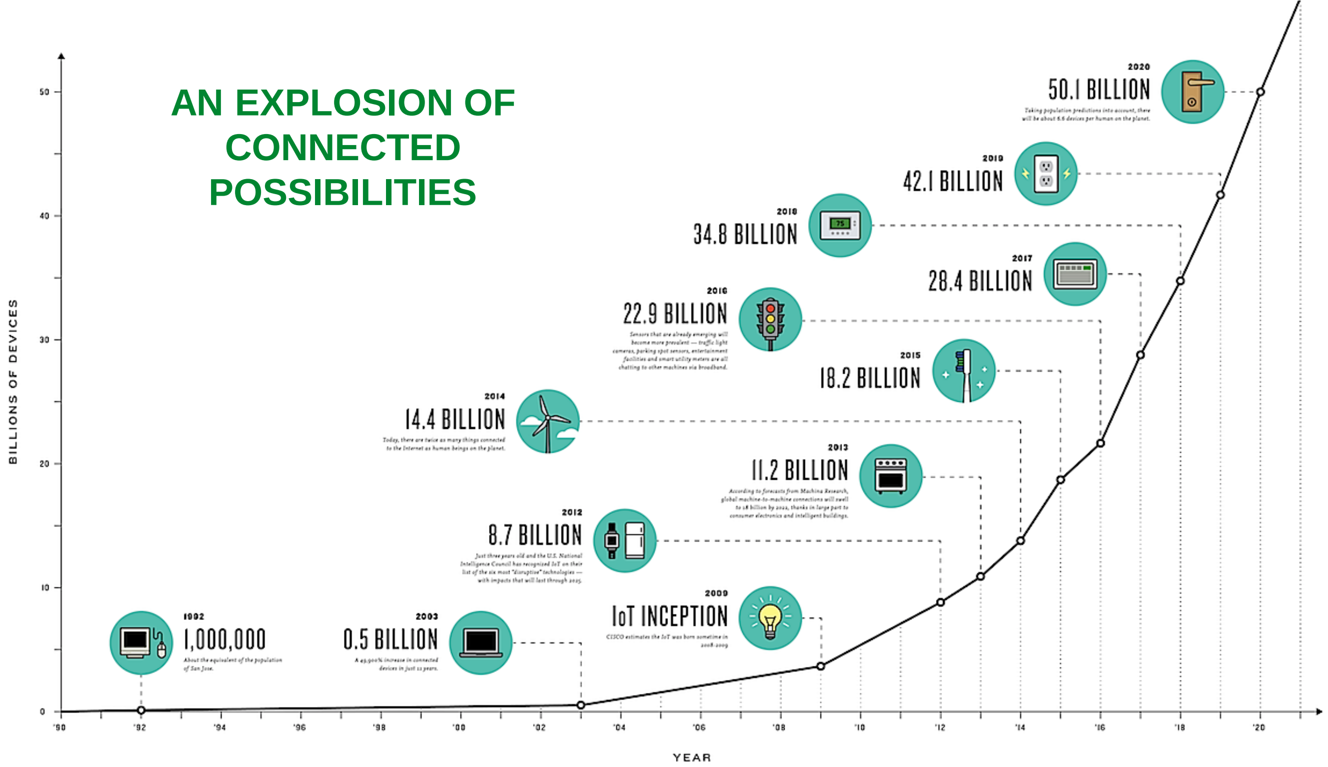
3 Developing a GDPR Program

4 The Record of processing activities, a practical use case

DIGITAL REVOLUTION IS HERE



ANALYSTS FORECAST ON IOT



About the equivalent of the population of San Jose.

A 49,900% increase in connected devices in just 11 years.

CISCO estimates the IoT was born sometime in 2008-2009

Just three years old and the U.S. National Intelligence Council has recognized IoT on their list of the six most "disruptive" technologies — with impacts that will last through 2025.

According to forecasts from Machina Research, global machine-to-machine connections will swell to 18 billion by 2022, thanks in large part to consumer electronics and intelligent buildings.

Today, there are twice as many things connected to the Internet as human beings on the planet.

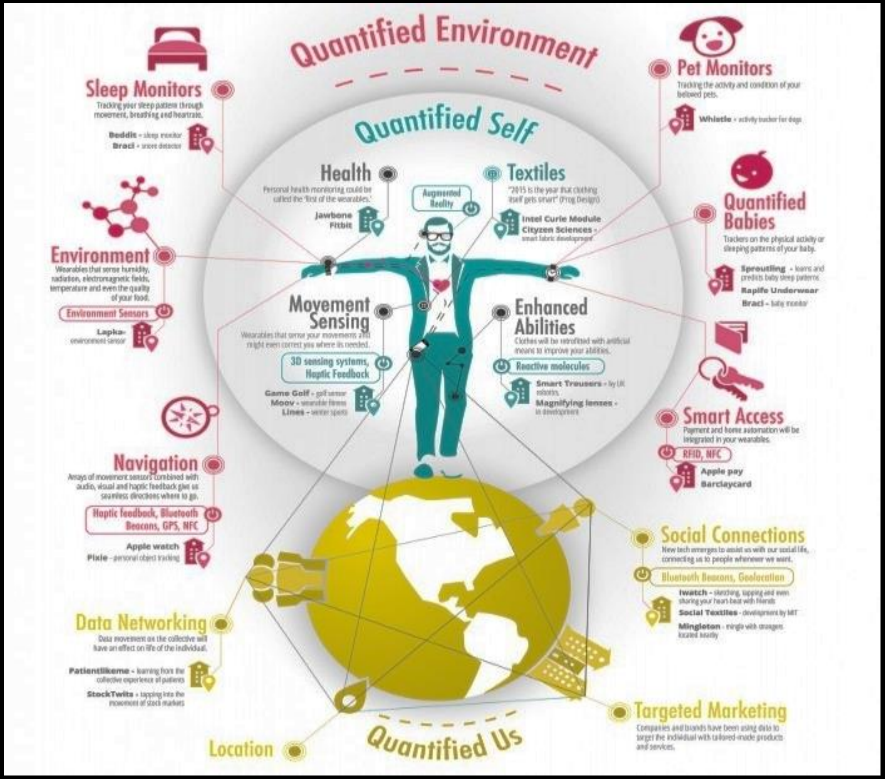
Sensors that are already emerging will become more prevalent — traffic light cameras, parking spot sensors, entertainment facilities and smart utility meters are all chatting to other machines via broadband.

Taking population predictions into account, there will be about 6.6 devices per human on the planet.

source: www.giovannipopolizio.it

QUANTIFIED SELF MOVEMENT

Also known as “**lifelogging**” and “**self-tracking**” is about acquiring huge amounts of data on the aspects of people’s daily lives. It concerns the amount of food consumed, the amount of steps taken, blood oxygen levels, sleep patterns, and much more. This movement is a “collaboration of users and tool makers who share an interest in self knowledge through self-tracking” (Wired Magazine, 2007)



Quantified Environment

Quantified Self

Sleep Monitors
Tracking your sleep pattern through movement, breathing and heartrate.
Beddit - sleep monitor
Braci - snore detector

Environment
Wearables that sense humidity, radiation, electromagnetic fields, temperature and even the quality of your food.
Environment Sensors
Lapka- environment sensor

Navigation
Arrays of movement sensors combined with audio, visual and haptic feedback give us seamless directions where to go.
Haptic feedback, Bluetooth Beacons, GPS, NFC
Apple watch
Pixie - personal object tracking

Health
Personal health monitoring could be called the 'first of the wearables.'
Jawbone
Fitbit

Augmented Reality

Textiles
"2015 is the year that clothing itself gets smart" (Frog Design)
Intel Curie Module
Cityzen Sciences - smart fabric development

Movement Sensing
Wearables that sense your movements and might even correct you where its needed.
3D sensing systems, Haptic Feedback
Game Golf - golf sensor
Moov - wearable fitness
Lines - sensor sports

Enhanced Abilities
Clothes will be retrofitted with artificial means to improve your abilities.
Reactive molecules
Smart Trousers - by UK robotics
Magnifying lenses - in development

Pet Monitors
Tracking the activity and condition of your beloved pets.
Whistle - activity tracker for dogs

Quantified Babies
Trackers on the physical activity or sleeping patterns of your baby.
Sproutling - learns and predicts baby sleep patterns
Rapife Underwear
Braci - baby monitor

Smart Access
Payment and home automation will be integrated in your wearables.
RFID, NFC
Apple pay
Barclaycard

Social Connections
New tech emerges to assist us with our social life, connecting us to people whenever we want.
Bluetooth Beacons, Geolocation
Iwatch - sketching, tapping and even sharing your heart beat with friends
Social Textiles - development by MIT
Mingleton - mingle with strangers located nearby

Data Networking
Data movement on the collective will have an effect on life of the individual.
Patientslikeme - learning from the collective experience of patients
StockTwits - tapping into the movement of stock markets

Targeted Marketing
Companies and brands have been using data to target the individual with tailored-made products and services.

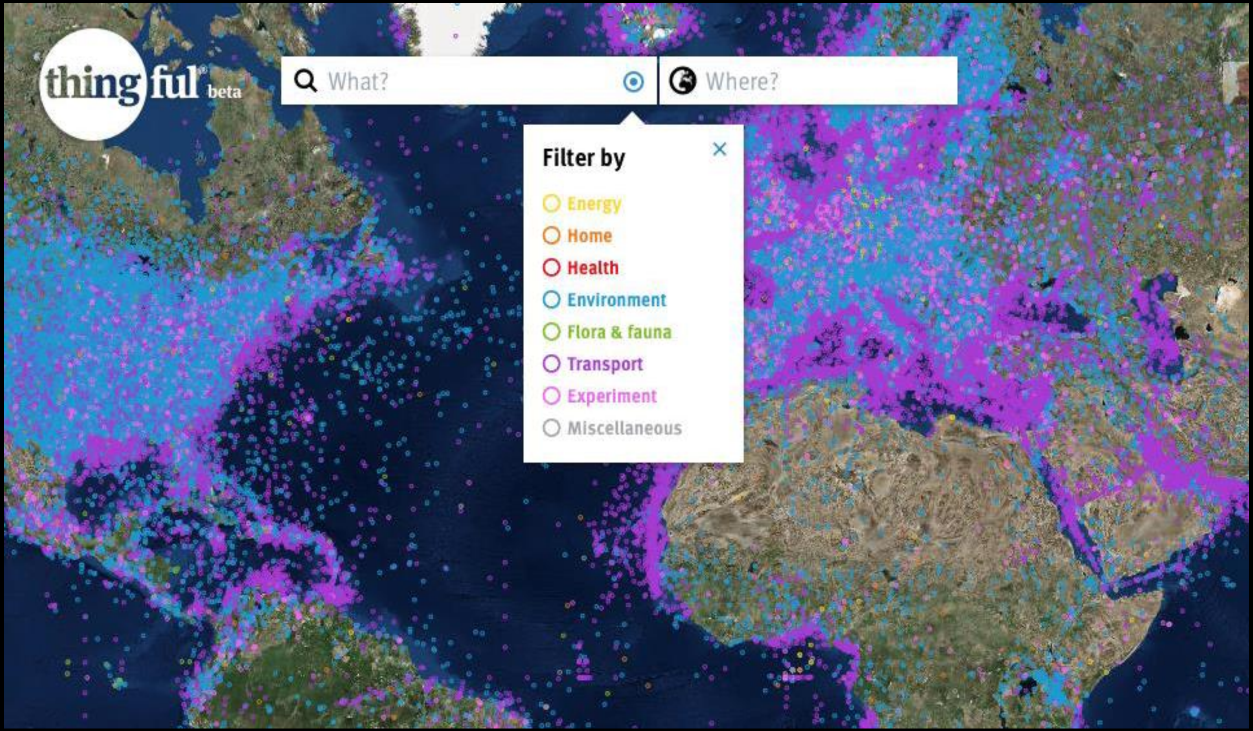
Location

Quantified Us

source: www.bananagun.nl

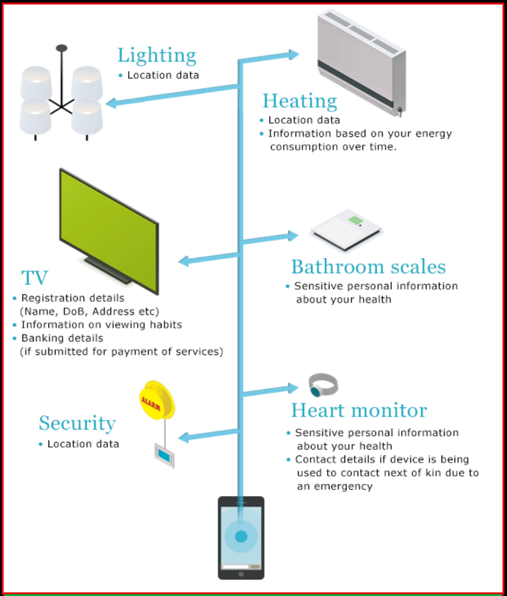
*“**Almost everything we do generates data**” - Gary Wolf* , Wired Magazine editor

THINGFUL BETA



Search engine for the internet of things (IoT), providing a unique geographical index of connected objects around the world, including eanergy, radiation, weather, and air quality devices as well as seismographs, iBeacons, ships, aircraft and even animal trackers.

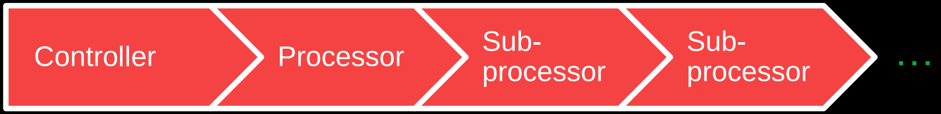
GDPR FOR BETTER PROTECTION AND CONTROL OF DATA


Lighting
• Location data
Heating
• Location data
• Information based on your energy consumption over time.
TV
• Registration details (Name, DoB, Address etc)
• Information on viewing habits
• Banking details (if submitted for payment of services)
Bathroom scales
• Sensitive personal information about your health
Security
• Location data
ALARM
Heart monitor
• Sensitive personal information about your health
• Contact details if device is being used to contact next of kin due to an emergency

don’t get me wrong, please

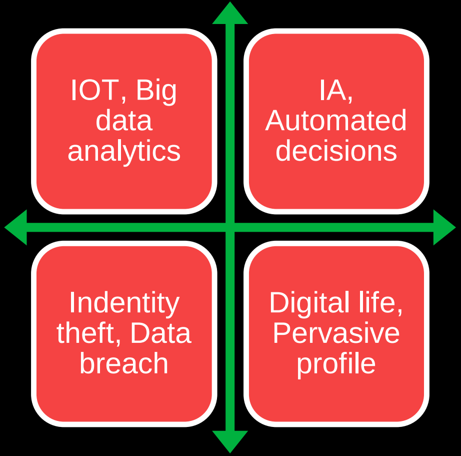
accidental mistakes, imprecise profile, breached data, altered data, lost data… could produce an harm to us

source: http://blogs.lse.ac.uks



Controller → Processor → Sub-processor → Sub-processor …

An extended digital-chain of processors added to a deeper digital person-profile increases the privacy risk



IOT, Big data analytics

IA, Automated decisions

Indentity theft, Data breach

Digital life, Pervasive profile

- Reputational damage
- **Discrimination**
- Decreased purchasing power
- **Blackmail**
- **Bullying**
- **Harassment**
- Economic loss
- Council service denied
- Professional harm
- **Political influence**
- Surveillance
- …

DO NOT CALL IT A PROJECT

GETTING GDPR-READY MEANS SETTING UP A PRIVACY MANAGEMENT SYSTEM, BEING ABLE TO SHOW IT AND KEEPING IT EFFECTIVE

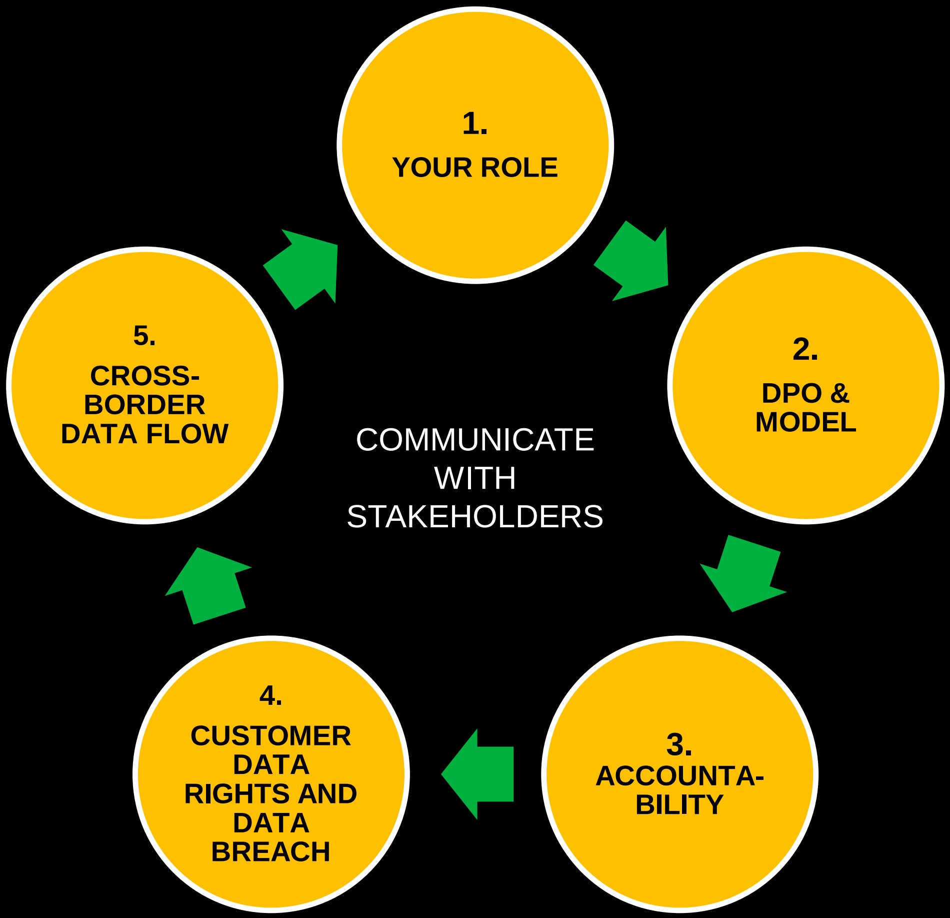
Processes *Data Breach Notification*, *Privacy Impact Assessment*, *Information request handling*, *Privacy Audit*, *Privacy Training, Privacy by Design:* these will be rolling activities whose effectiveness should be measurable to assess the effectiveness of the whole Management System

Policies and Controls *Governance Framework*, from guidelines to procedures to records to audit trails to *organizational and technological measures*

People *Beyond the DPO*, where required, *further roles are necessary* in a company to distribute responsibilities: there is no one-model-fit-all, each company should evaluate the most appropriate *privacy organizational model*.

A management system is a “living” entity which adapts to business context (new markets-products-services, M&A, demerge, law/policies changes, …) and improves over time

TOP 5 PRIORITIES



DEFINE YOUR PRIORITIES ANSWERING THE FOLLOWING QUESTIONS

1. Do I know **my role** – as Controller or Processor – for all the processing activities?
2. Does my current **privacy organizational model** fit the GDPR?
3. Can I **show accountability** in all processing activities?
4. Am I ready to face **data subjects requests** exercising their rights and to respond to data breach?
5. Are all my **cross-border data flows** compliant with GDPR?

DIFFERENT POINTS OF VIEW?

OR CONVERGING NEEDS?

DATA PROTECTION AUTHORITY

Is the Governance Framemork complete? Are practices aligned to it? Are roles assigned? Can you show evidences of effectiveness? Is a remediation plan defined for breaches?

CUSTOMERS

Can you delete my data? Why are you contacting me without consent? Why did you disclose my data I erased some time ago? Who are the third parties processing my data, and where?

GDPR PROGRAM MANAGER

Are task-ownerships assigned? Are task dependencies clear? Are goals achievable? Is the Program endorsed adequately? Is the working team skilled? Are criticalities addressed?

PRIVACY OFFICERS, LEGAL , COMPLIANCE

Are privacy risks assessed? Are employees aware of their duties and responsibilities? Are company practices on data compliant with policies and notices? How long data are retained?

CTO, CDO CSO, CISO

Do applications store audit trails to enforce breach prevention and management? Are user access rights and profiles validated? Is data protected adequately from collection to erasure?

7 DON'TS YOU SHOULD KNOW

Delay the awareness to the Board

Run separate initiatives

Don't review your organizational model

Use a sledge hammer to crack a walnut

Focus on privacy, postponing security

Assess and test the processing activities customer-faced

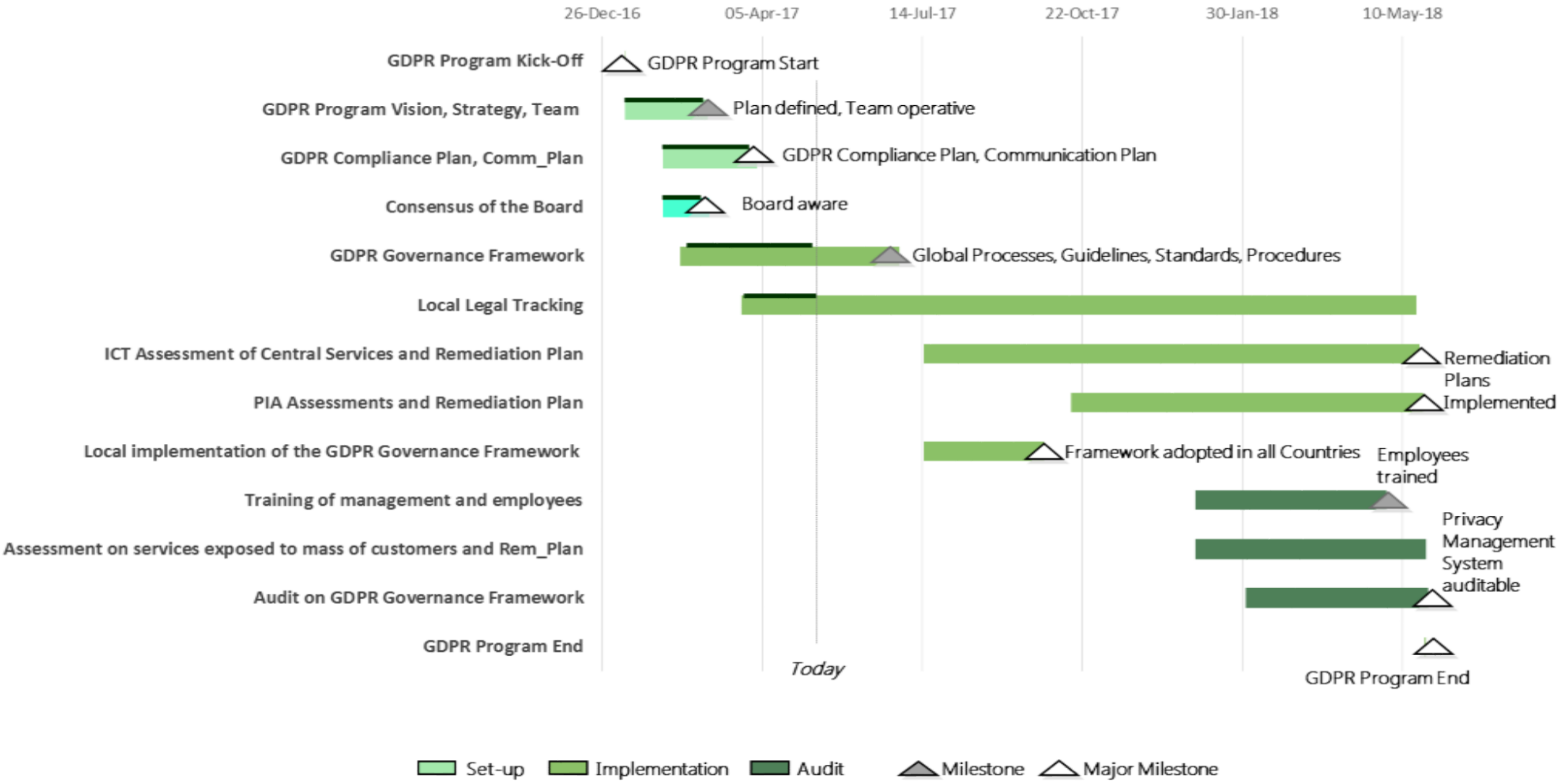
Underestimate the importance of a skilled team

GDPR PROGRAM SAMPLE TEAM

** Illustrative GDPR extended working team for a large company, in smaller companies roles and responsibilities could be aggregated*

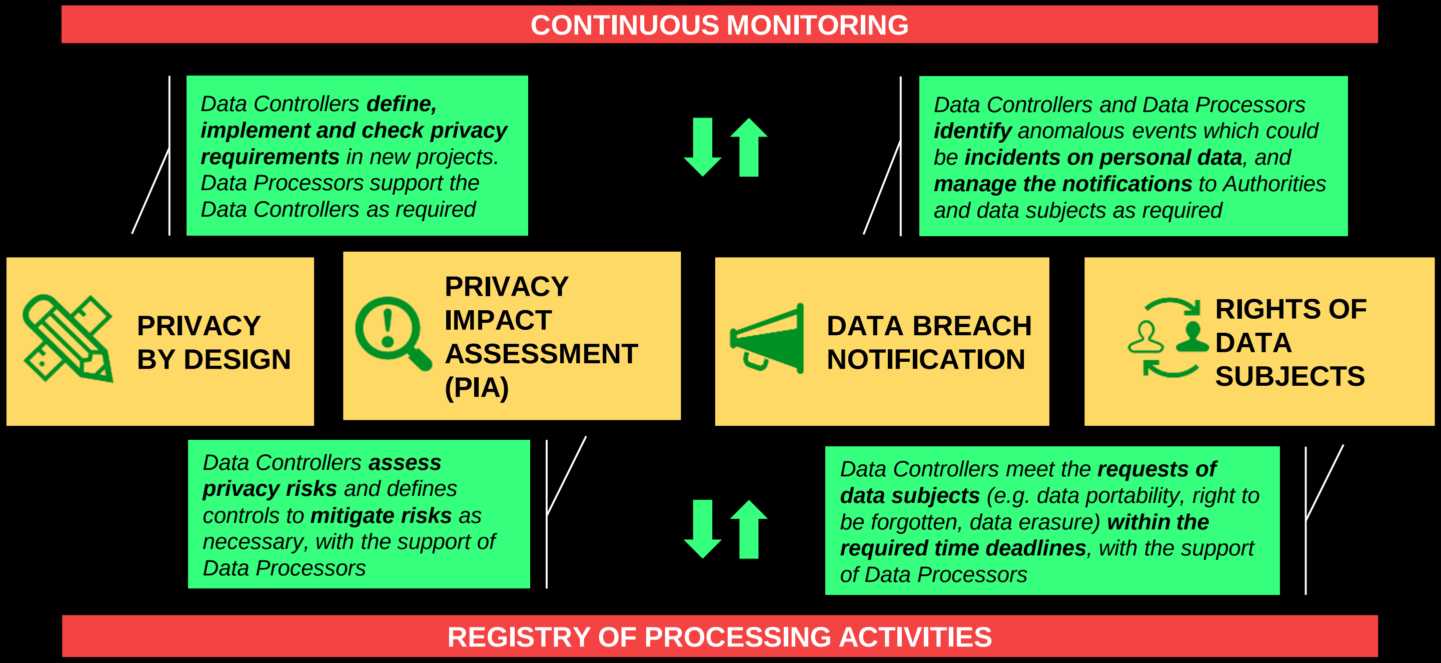
	People *	Role *
Steering Committee and Sponsors	– **Board, Heads of Departments** and other **Stakeholders** (e.g. Mktg, HR, Compliance, Legal, ICT, Ops.)	– Vision, Strategy and Goals Setting – Endorsment and Program Visibility
Program Coordination and Quality Assurance	– **GDPR Program Manager**	– Coordination, communications, escalation management – Interface towards Stakeholders and the Working Team – Support the DPO for Program quality assurance
Program Auditing and Approval	– **Data Protection Office(r)** – **Internal Audit** – **Specialized 3 Parties and consultants**	– DPO: check and approval of intermediate/final deliverables – IA, 3Ps: if present, support DPO for ensuring the auditability of the Privacy Management System
Program Implementation	– **Chief Privacy Officer** – **Privacy and Security Practitioners** – **Company Areas Privacy Champions** – **Specialized 3 Parties and consultants**	– CPO: lead and coordinate and supervise the working team, interface with DPO and Program Manager – Practitioners, i.e. working team: develop the framework documentation, perform the info gathering (interviews, workshops), deliver assessments and remediation plans – Areas Champions: support the working team, sharing and preliminary validation of partial outcomes – 3Ps, Consultants: support the working team

GDPR PROGRAM SAMPLE PLAN



GDPR GOVERNANCE FRAMEWORK "IN RUNNING"

Periodic assessments *to check that companies implement governance framework correctly, with* ***remediation plans*** *as necessary*



CONTINUOUS MONITORING

Data Controllers ***define, implement and check privacy requirements*** *in new projects. Data Processors support the Data Controllers as required*

Data Controllers and Data Processors ***identify*** *anomalous events which could be* ***incidents on personal data****, and* ***manage the notifications*** *to Authorities and data subjects as required*

PRIVACY BY DESIGN

PRIVACY IMPACT ASSESSMENT (PIA)

DATA BREACH NOTIFICATION

RIGHTS OF DATA SUBJECTS

Data Controllers ***assess privacy risks*** *and defines controls to* ***mitigate risks*** *as necessary, with the support of Data Processors*

Data Controllers meet the ***requests of data subjects*** *(e.g. data portability, right to be forgotten, data erasure)* ***within the required time deadlines****, with the support of Data Processors*

REGISTRY OF PROCESSING ACTIVITIES

Companies keep their ***Registry of processing activities updated****, documenting any relevant changes as new activities on personal data (privacy by design, PIA if required), new suppliers, new applications, requests of data subjects, etc.*

THE REGISTRY IN YOUR PRIVACY GOVERNANCE FRAMEWORK

Registry *is the* ***key element*** *of the Privacy Governance Framework and has* ***tight interactions with*** *other* ***framework elements***

Registry of processing activities

Records of processing activities carried out by company/holding on personal data

Privacy Impact Assessment (PIA) & Monitoring

Processing operations requiring PIA are highlighted in the Registry by the DPO/GDPR Central Team, as well as PIA score and date of achievement. Information within the Registry are used to plan monitoring plans

Data breach notification

Information within the Registry are useful to manage data breach notification, e.g. data, IT applications, suppliers, location possibly impacted; and can be useful for the breach management as well

Privacy and Security by design

Privacy and security requirements documented for new projects, products, services could update the content of the Registry

Contracts management

Information within the Registry are useful for defining the content of privacy requirements for, contract clauses with, appointment as Processors of Suppliers involved in processing activities

Data Subject Request

Information within the Registry allow to know where data is, how it is used and by whom, which supplier is involved, where the data is transferred, etc.

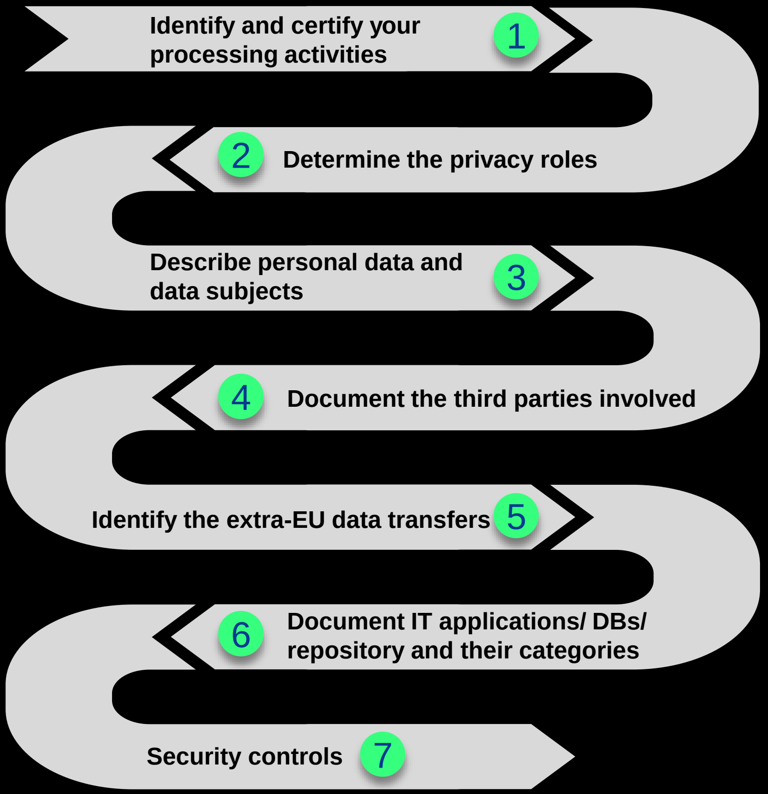
STEPS TO FILL-IN THE REGISTRY

1 **Description of the processing activity** carried out by the company on personal data,

3 Description of the **category of personal data** processed and of **data subject** impacted

5 **Extra-EU countries** where personal data is transferred by the company, and **legitimate basis** for allowing such transfer

7 **Security measures** adopted to secure the processing activity, personal **data retention** period and **data erasure measures** adopted



Identify and certify your processing activities 1

2 **Determine the privacy roles**

Describe personal data and data subjects 3

4 **Document the third parties involved**

Identify the extra-EU data transfers 5

6 **Document IT applications/ DBs/ repository and their categories**

Security controls 7

2 Chain of privacy accountable roles (**Controller, Main Contractor, Role of the company**) in relation to the processing activity. Remark: not all the roles are always present (e.g. Main Contractor)

4 **Third Parties** to whom part of the processing activity is delegated by the company, **according to a written contract**

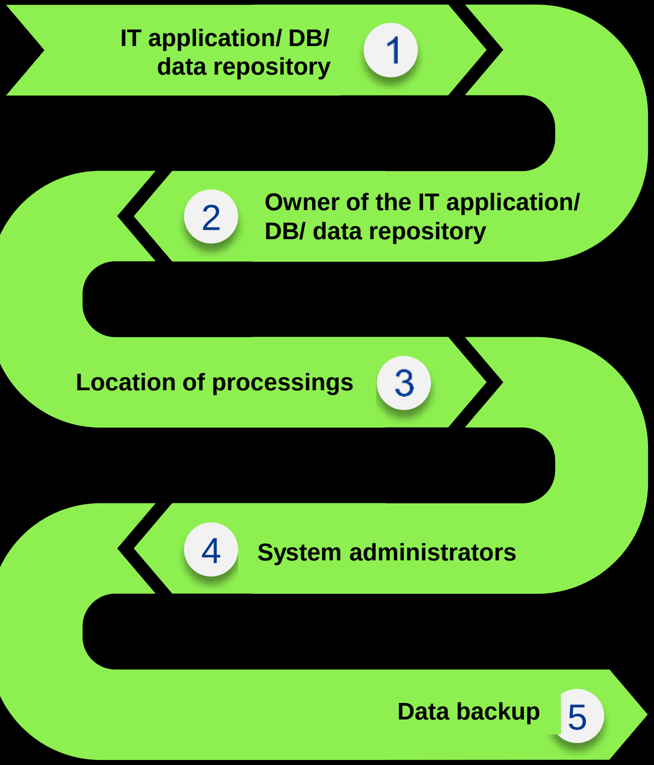
6 **IT applications/ DBs and repositories** used within the processing activity. Remark: only IT applications/ DBs and repositories **under the direct responsibility of the company** (not of the customer) shall be listed

REGISTRY - IT APPLICATIONS-DBS-REPOSITORIES

1 Vendor, name, version of the IT application/ DB/ data repository
Remark: only IT applications/ DBs/ data repositories under the direct responsibility of the company shall be listed, not of the Customer

3 Location of the IT application/ DB/ data repository

5 Contact detail of owner of data backup, retention period and location of data backup.



IT application/ DB/ data repository 1

2 Owner of the IT application/ DB/ data repository

Location of processings 3

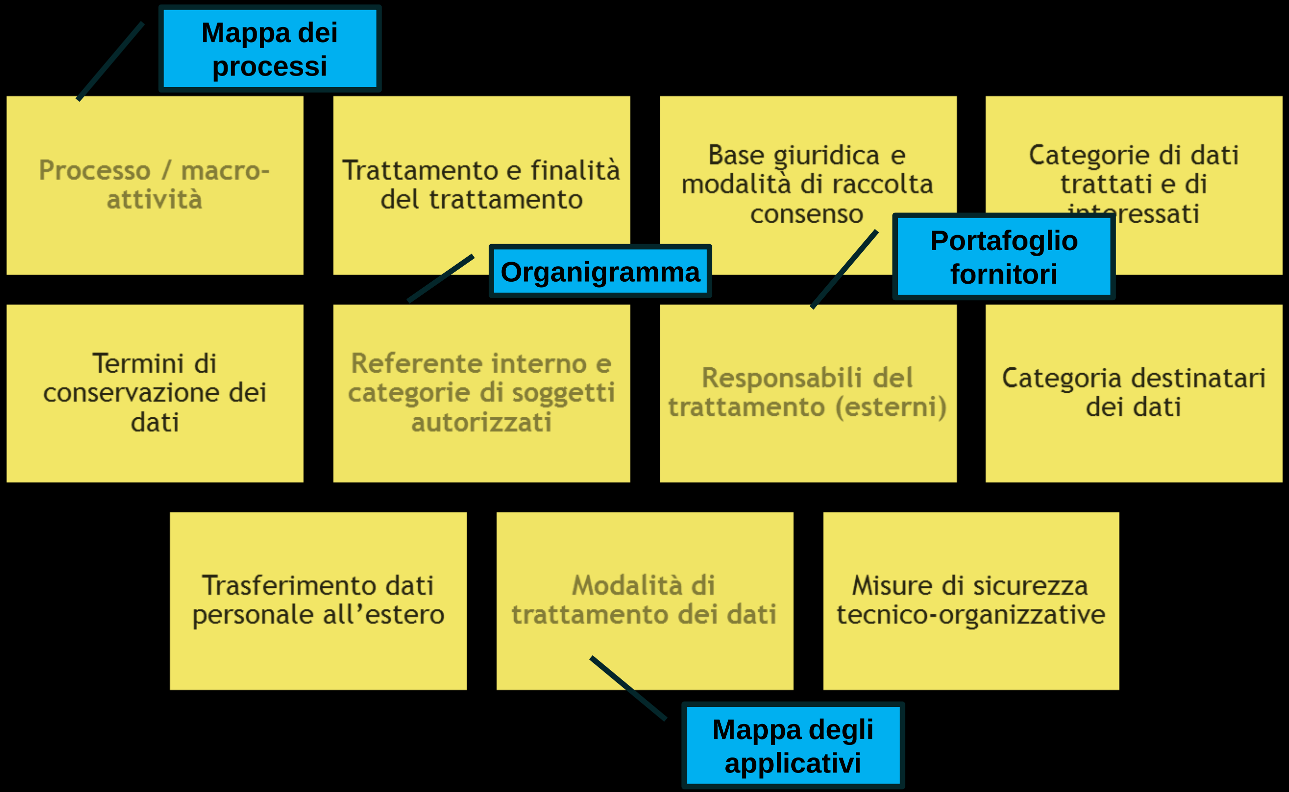
4 System administrators

Data backup 5

2 Name and contact details of the owner

4 Contact detail of system administrator and log retention period. Remark: this cluster of information is NOT mandatory for non-Italian companies

REGISTRY – INTEGRATION WITH COMPANY FRAMEWORK



Mappa dei processi

Processo / macro-attività

Trattamento e finalità del trattamento

Base giuridica e modalità di raccolta consenso

Categorie di dati trattati e di interessati

Organigramma

Portafoglio fornitori

Termini di conservazione dei dati

Referente interno e categorie di soggetti autorizzati

Responsabili del trattamento (esterni)

Categoria destinatari dei dati

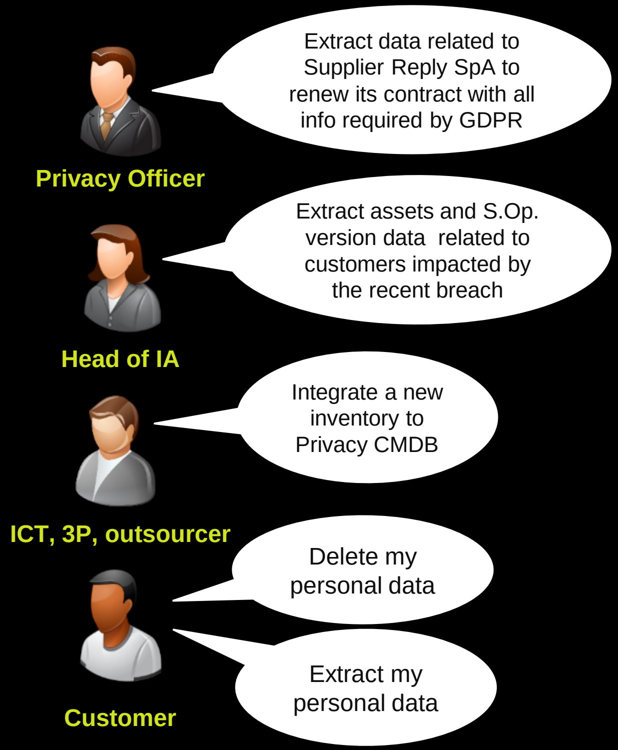
Trasferimento dati personale all'estero

Modalità di trattamento dei dati

Misure di sicurezza tecnico-organizzative

Mappa degli applicativi

USE CASE - PRIVACY ASSET INVENTORY



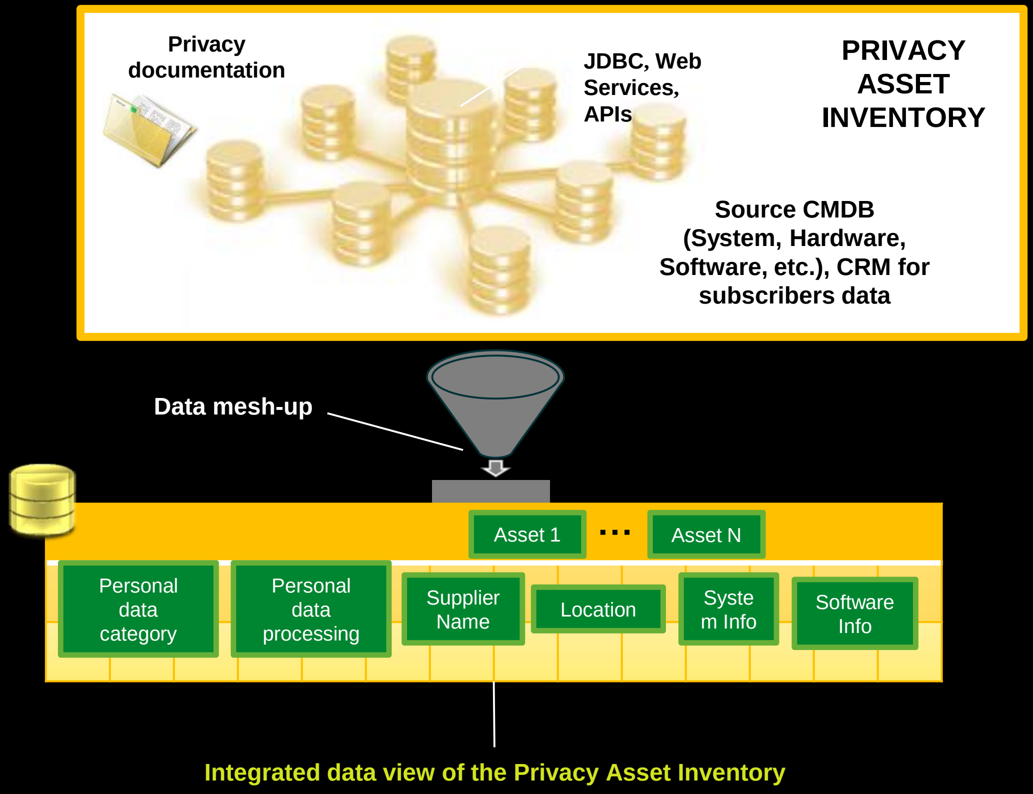
Privacy Officer: Extract data related to Supplier Reply SpA to renew its contract with all info required by GDPR

Head of IA: Extract assets and S.Op. version data related to customers impacted by the recent breach

ICT, 3P, outsourcer: Integrate a new inventory to Privacy CMDB

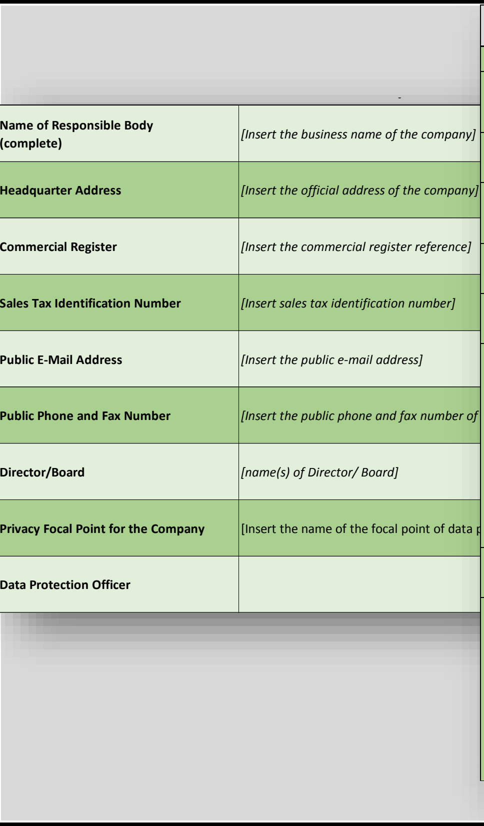
Customer: Delete my personal data

Customer: Extract my personal data

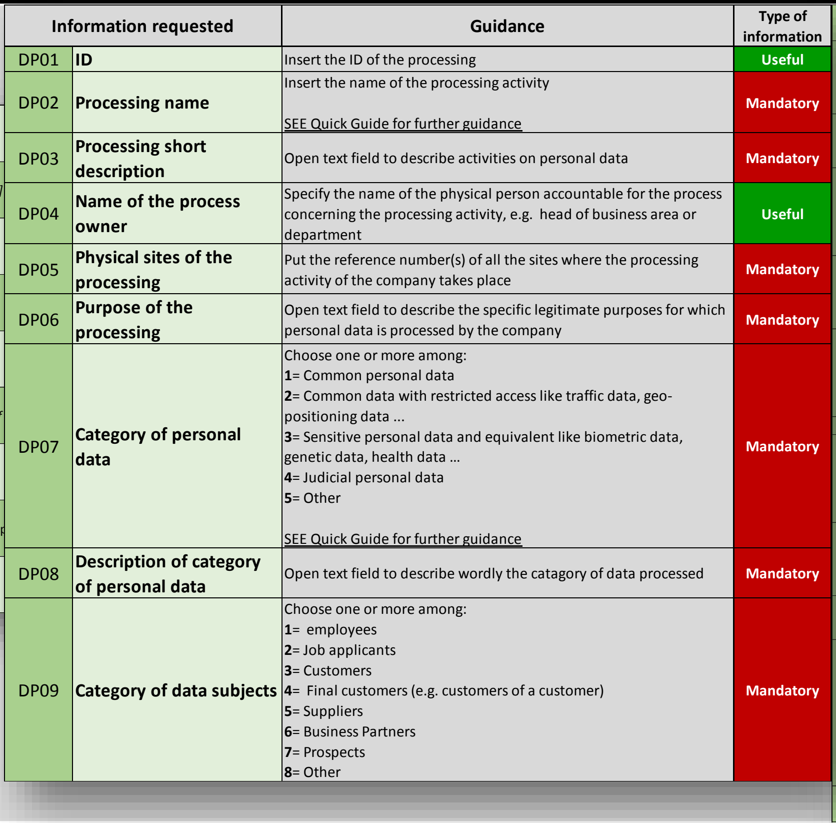


Integrated data view of the Privacy Asset Inventory

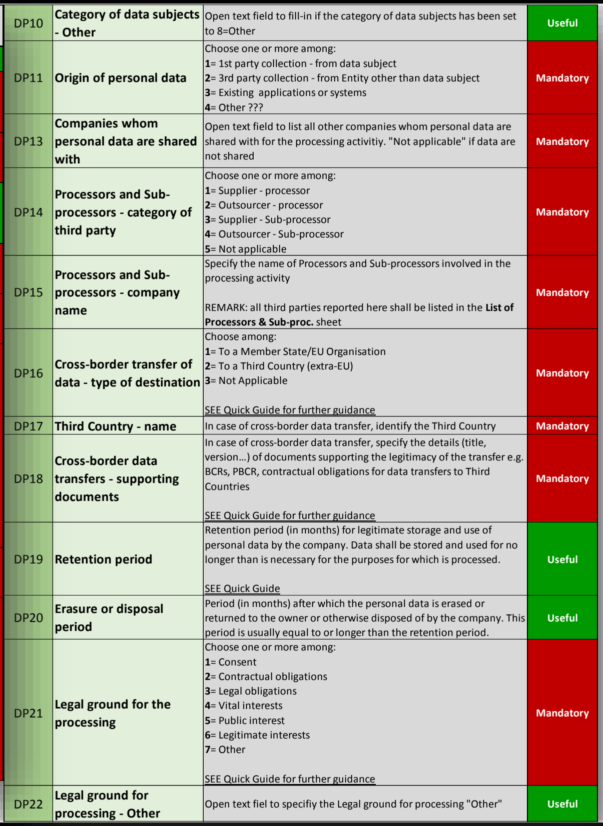
REGISTRY – MAKE OR BUY?



Name of Responsible Body (complete)	*[Insert the business name of the company]*
Headquarter Address	*[Insert the official address of the company]*
Commercial Register	*[Insert the commercial register reference]*
Sales Tax Identification Number	*[Insert sales tax identification number]*
Public E-Mail Address	*[Insert the public e-mail address]*
Public Phone and Fax Number	*[Insert the public phone and fax number of*
Director/Board	*[name(s) of Director/ Board]*
Privacy Focal Point for the Company	[Insert the name of the focal point of data p
Data Protection Officer	

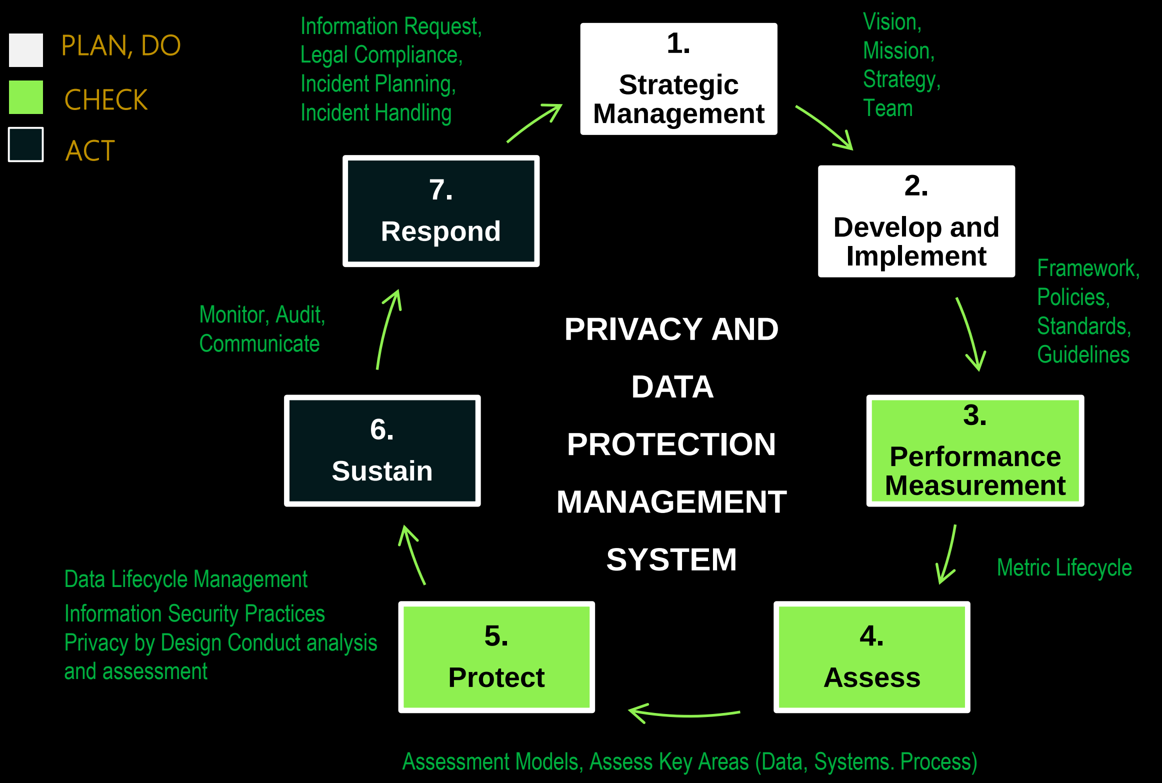


Information requested		Guidance	Type of information
DP01	ID	Insert the ID of the processing	Useful
DP02	Processing name	Insert the name of the processing activity SEE Quick Guide for further guidance	Mandatory
DP03	Processing short description	Open text field to describe activities on personal data	Mandatory
DP04	Name of the process owner	Specify the name of the physical person accountable for the process concerning the processing activity, e.g. head of business area or department	Useful
DP05	Physical sites of the processing	Put the reference number(s) of all the sites where the processing activity of the company takes place	Mandatory
DP06	Purpose of the processing	Open text field to describe the specific legitimate purposes for which personal data is processed by the company	Mandatory
DP07	Category of personal data	Choose one or more among: **1**= Common personal data **2**= Common data with restricted access like traffic data, geo-positioning data ... **3**= Sensitive personal data and equivalent like biometric data, genetic data, health data ... **4**= Judicial personal data **5**= Other SEE Quick Guide for further guidance	Mandatory
DP08	Description of category of personal data	Open text field to describe wordly the catagory of data processed	Mandatory
DP09	Category of data subjects	Choose one or more among: **1**= employees **2**= Job applicants **3**= Customers **4**= Final customers (e.g. customers of a customer) **5**= Suppliers **6**= Business Partners **7**= Prospects **8**= Other	Mandatory



DP10	Category of data subjects - Other	Open text field to fill-in if the category of data subjects has been set to 8=Other	Useful
DP11	Origin of personal data	Choose one or more among: **1**= 1st party collection - from data subject **2**= 3rd party collection - from Entity other than data subject **3**= Existing applications or systems **4**= Other ???	Mandatory
DP13	Companies whom personal data are shared with	Open text field to list all other companies whom personal data are shared with for the processing activitiy. "Not applicable" if data are not shared	Mandatory
DP14	Processors and Sub-processors - category of third party	Choose one or more among: **1**= Supplier - processor **2**= Outsourcer - processor **3**= Supplier - Sub-processor **4**= Outsourcer - Sub-processor **5**= Not applicable	Mandatory
DP15	Processors and Sub-processors - company name	Specify the name of Processors and Sub-processors involved in the processing activity REMARK: all third parties reported here shall be listed in the **List of Processors & Sub-proc.** sheet	Mandatory
DP16	Cross-border transfer of data - type of destination	Choose among: **1**= To a Member State/EU Organisation **2**= To a Third Country (extra-EU) **3**= Not Applicable SEE Quick Guide for further guidance	Mandatory
DP17	Third Country - name	In case of cross-border data transfer, identify the Third Country	Mandatory
DP18	Cross-border data transfers - supporting documents	In case of cross-border data transfer, specify the details (title, version...) of documents supporting the legitimacy of the transfer e.g. BCRs, PBCR, contractual obligations for data transfers to Third Countries SEE Quick Guide for further guidance	Mandatory
DP19	Retention period	Retention period (in months) for legitimate storage and use of personal data by the company. Data shall be stored and used for no longer than is necessary for the purposes for which is processed. SEE Quick Guide	Useful
DP20	Erasure or disposal period	Period (in months) after which the personal data is erased or returned to the owner or otherwise disposed of by the company. This period is usually equal to or longer than the retention period.	Useful
DP21	Legal ground for the processing	Choose one or more among: **1**= Consent **2**= Contractual obligations **3**= Legal obligations **4**= Vital interests **5**= Public interest **6**= Legitimate interests **7**= Other SEE Quick Guide for further guidance	Mandatory
DP22	Legal ground for processing - Other	Open text fiel to specifiy the Legal ground for processing "Other"	Useful

PRIVACY PROGRAM AFTER MAY ’18



□ PLAN, DO

🟩 CHECK

■ ACT

1. Strategic Management

Vision, Mission, Strategy, Team

2. Develop and Implement

Framework, Policies, Standards, Guidelines

3. Performance Measurement

Metric Lifecycle

4. Assess

Assessment Models, Assess Key Areas (Data, Systems. Process)

5. Protect

Data Lifecycle Management
Information Security Practices
Privacy by Design Conduct analysis and assessment

6. Sustain

Monitor, Audit, Communicate

7. Respond

Information Request, Legal Compliance, Incident Planning, Incident Handling

PRIVACY AND DATA PROTECTION MANAGEMENT SYSTEM

By May 2018 you will have likely implemented most part of the framework, and started checking it. No matter why and how, what you should focus on is **keeping it going as a rolling process** which will **improve over time and produce** all the **accountability trails** required by the GDPR.

It is not a 12vmonths exercise, **it is a new regime of data protection** looming on EU and beyond.