GDPR

Making it Easy

16th March 2018

Ing. Joseph Caruana

Data in GDPR context is Personal Data

Tuning Fork

It’s all about the Privacy of the Data Subject

Not an IT Fix
Not a Legal Fix

Tuning Fork proposes compliance by Design and Default

Tuning Fork

You should focus on growing your business and not on GDPR compliance issues

The R.I.P. approach

Reduce, Inhibit, Pseudonymise

Protecting the privacy of the data subjects must be by design and by default:

- By integrated it in your operations effectively
- Through setting operational, procedural and technical measures

Tuning Fork Input

Mr. Reasonable Customer

- Do you **store** data or do you also **process** it?

- By Storage, I mean: – on Network, Cloud, Databases, Servers, Internet, e-mail, other software, voice recordings, paper (hard copy information,), old files in stores and any other media that stores personal data

Storage Locations

- Advise me in which **countries** is all this data **stored** in or **accessible** from

- **Where are the physical servers** of the cloud services with my data located (are or where in the past 12 months)

Servers and Jurisdictions

- Please **provide** me with a copy of, or access to, my personal data that you have or are processing.

- Please provide a list of all third parties with whom you have (**or may have**) shared or disclosed my personal data.

Data at Third Parties

- Please advise how long you store my personal data, and if **retention** is based upon the **category of personal data,** please identify how long each category is retained.

Retention Policy

- If you are additionally collecting personal data about me from **any source other than me**, please provide me with all information about their source, (*as referred to in Article 14 of the GDPR*).

- I would like to know, with evidence, whether or not my personal data has been **disclosed inadvertently** by your company in the past, or as a result of a security or privacy breach.

Controls for disclosure

- Have you had any circumstances in which employees or contractors have been dismissed, and/ or been charged under criminal laws for accessing **my personal data** inappropriately, or if you are unable to determine this, **or of any customers**, in the past twelve months.

Legal Action

- We will established pathways , SOPs for these eventualities, both for staff as well as clients
- We will establish and define a timeframe for **data retention based on** for how long do we need this data? And why?

- We will map data (Virtual and Actual) locations for both storage and processing, including categories and retention periods
- Link Data location to Countries and jurisdictions
- Prepare templates to submit to client (*using EU established/approved templates*)

Tuning Fork Input

- Identify and maintain mechanism for third party lists and locations of access to data
- Identify external sources of personal data
- Design, define and document breach policy and corrective action mechanism

Tuning Fork Input

Mr. Super Annoyed Client

- **Rectify** data that is inaccurate
- **Erasure** all date that does not want to consent to anymore
- **Restrict** data to be used
- **Transfer** data from one controller to another without any hindrances
- **Object** to usage of data for public/legal interest or direct marketing

Data Subjects right (pivotal to GDPR)

- Please provide me with a **detailed accounting of the specific uses** that you have made, are making, or will be making of my personal data.

Audit Trail

- Tell me in which **jurisdictions** these **third parties** with whom you have or may have shared my personal data, have stored or can access my personal data.

- Please provide basis of legal grounds for transferring my personal data to these jurisdictions. Where you have done so, on the basis of appropriate safeguards, ***please provide a copy.***

Jurisdictions

- I would like to know what **safeguards** have been put in place in relation to these third parties that you have identified in relation to the transfer of my personal data.

Safeguards

- When there was a **breach** please tell me:
  - a general description of what occurred
  - the date and time of the breach (or the best possible estimate);
  - the date and time the breach was **discovered**;
  - the source of the breach (either your own organization, or a third party to whom you have transferred my personal data);
  - details of my personal data that was disclosed;

Breach Management

- When there was a breach please tell me:
  - details of my personal data that was disclosed;
  - your company's assessment of the risk of harm to myself, as a result of the breach;
  - a description of the measures taken or that will be taken to prevent further unauthorized access to my personal data;
  - contact information so that I can obtain more information and assistance in relation to such a breach,
  - information and advice on what I can do to protect myself against any harms, including identity theft and fraud.

Breach Management

- If you are not able to state with any certainty whether such an exposure has taken place, through the use of appropriate technologies, please advise what mitigating steps you have taken, such as

  - Encryption of my personal data;
  - Data minimization strategies;
  - Anonymization or pseudonymizing;
  - Any other means

- In regards to employees and contractors, please advise what technologies or business procedures do you have in place to ensure that individuals within your organization will be **monitored** to ensure that they do not **deliberately or inadvertently** disclose personal data outside your company, through e-mail, web-mail or instant messaging, or otherwise.

Procedures

- Reduce or eliminate access or identification
- Research third party base jurisdictions
- System for Data usage mapping with audit trail
- Design and implementation of safeguards, documented, contractual or physical
- Breach Policy, avoidance and corrective action process
- Full IT support for encryption
- HR policies, procedures and declarations

Tuning Fork Input

Mr. Pain in the B Customer

- Is necessary when there is the likeliness of HIGH risk to the rights of the DS.

- The data controller decides or envisages this risk (Particularly in automated /systematic data collection)

- Please advise as to what **training** and **awareness** measures you have taken in order to ensure that employees and contractors are accessing and processing my personal data in conformity with the General Data Protection Regulation.

Provide formal certified Training to employees and suppliers on

- Understanding what data is (in terms of the GDPR)
- Work and protect data (***and data subject***) at the same time

Tuning Fork Input

- If you are making automated decisions about me, including profiling, (*whether or not because of Article 22 of the GDPR*), please provide me with information concerning the **basis for the logic** in making such automated decisions, and the significance and consequences of such processing.

- I would like to know your **information policies** and standards that you follow in relation to the safeguarding of my personal data, such as whether you adhere to ISO27001 for information security

- Please inform me how and whether you have backed up my personal data to tape, disk or other media, and where it is stored and how it is secured, including what steps you have taken to protect my personal data from loss or theft, and whether this includes encryption

- Please advise how and whether you have in place any technology which allows you with reasonable certainty to know whether or not my personal data has been disclosed, including but not limited to the following:
  - Intrusion detection systems;
  - Firewall technologies;
  - Access and identity management technologies; Database audit and/or security tools;
  - Behavioral analysis tools, log analysis tools, or audit tools;

- Is needed for organizations which handle data on a large scale.
- The DPO can decide if his data administration is considered on a large scale or not:
  - Depending on the number of employees
  - Volume of data used/administrated
  - Frequency of collecting data
  - Volume of colleting data

- Design and Delivery of certified training and awareness programmes
- Logic mapping of automated decisions
- Design of Information Policies
- Implement ISO27001 to certification
- Design of Data Backup Policies and Procedures
- Ethical Hacking to tests IT system vulnerability to hacking or data damage, loss or extraction
- ***Train or BE your back-office DPO***

Tuning Fork Input

- *Finding the dispersed data!!!*

Tuning Fork

Don’t Panic as it will not solve anything

The fact that tomorrow's crises will to some extent be dealt with using today's tools, does not mean that we should be complacent about being prepared

Questions