GDPR in practice for small & medium enterprises

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Internationalization through e-Commerce 2018
Zurich, 21 June 2018

GDPR

- On 25 May 2018, the **General Data Protection Regulation** has become the main body of privacy law **directly applicable** in all Europe («**GDPR**»).

- Among various novelties, the GDPR has introduced:
  - ✓ **New privacy rights** for data subjects;
  - ✓ **More extensive** information duties for businesses;
  - ✓ A higher standard for **consent**;
  - ✓ New organizational requirements for businesses.

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

(Some) FAQs on the GDPR

- We will try to answer the most frequently asked questions on the new rules:

1. Is **Double Opt-In** necessary to comply with the GDPR?
2. Can we send marketing email(s) to customers without their prior consent (**soft spam**)?
3. What is the statutory **retention period** for personal data?
4. In case of an user's request to erase their data («**right to be forgotten**»), shall we erase all data?
5. Shall we designate a **Data Protection Officer**?

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Double opt in: is it mandatory?

- Double opt-in is an email subscription process consisting of **two steps**:
  1. The user submits their email address via the subscription form on the website; and, subsequently,
  2. The user receives an e-mail where they have to **confirm** their will to be added to the mailing list.
- Under the GDPR, there is no requirement to apply a double opt-in process.

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Double opt in: is it mandatory? (2)

- Nonetheless, «double opt in» brings **benefits** both from a regulatory and marketing perspective:
  1. The fact that users confirms their subscription by clicking on a link in the confirmation email is **strong evidence** of their consent to receive newsletters and marketing emails;
  2. It appears more abiding to the **privacy by design** principle;
  3. Double opt in eventually leads to a narrower, **higher quality database** (no inadvertent or fraudulent opt-ins).

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Soft spam: is it allowed?

- At specific conditions, EU law allows merchants to submit commercial e-mail communications to their customers without prior consent («**E-privacy Directive**» 2002/58/EC).

"where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, **in accordance with Directive 95/46/EC**, the same natural or legal person **may use** these electronic contact details for direct marketing of its own **similar products or services** provided that customers clearly and distinctly **are given the opportunity to object, free of charge and in an easy manner**, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use" **(Art. 13 of 2002/58/EC**

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Soft spam: is it allowed? (2)

- Soft spam is possible with **customers**, not with users.
- Within a short period, the E-privacy Directive should be **repealed** by the **E-Privacy Regulation**, which is currently pending approval by the EU institutions.
- The current draft of the E-Privacy Regulation includes a provision on soft spam that is quite similar to the wording of the E-privacy Directive currently in force. However, it refers to «end users» not to «customers» (wider scope?).

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Soft spam: is it allowed? (3)

- The recitals to the proposed E-privacy Regulation point out: «*it is reasonable to allow the use of e-mail contact details within the context of an existing customer relationship for the offering of similar products or services*» (recital n. 33).

- The GDPR*: "the legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. Such legitimate interest could exist for example …in situations such as* ***where the data subject is a client*** (recital n. 47).

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Retention period for personal data

- Thet GDPR states personal data shall be kept for **no longer** than is necessary for the purposes for which it is being processed.

- The GDPR also requires that websites report in their **privacy policy** «*the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;*» (art. 13).

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Retention period for personal data (2)

- The period of personal data retention should be limited to a strict minimum and **time limits** should be established by the data controller for deletion of the records or for a periodic review (Recital n. 39).
- Businesses may need to retain some types of personal data for a specific period to comply with **financial** or **other regulations** in their own country.

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Retention period for personal data (3)

- To determine the appropriate retention period for personal data, the data controller will take into account **multiple factors**. Such criteria will also include:

  ✓ The purpose for which the controller holds such personal data;

  ✓ The type of ongoing **relationship** with the concerned user or customer (how often the user logs into their site account, whether users continue to receive marketing communications, how regularly they browse or buy on the site, etc.);

  ✓ **Legitimate business interests**.

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

The right to be forgotten (1)

- Following the path of the European Court of Justice, the GDPR introduces a right for individuals to have personal data **erased** at specific conditions.
- Data subjects can make a request for erasure verbally or in writing. Businesses have one month to respond to a request.
- The right is **not** absolute and only applies in certain circumstances.

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

The right to be forgotten (2)

- There are various derogations when the right to be forgotten does **not** apply. For instance:

1. For compliance with a **legal obligation** which requires processing or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and/or
2. For the establishment, exercise or defence of **legal claims**.

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

The right to be forgotten (3)

- Where the controller has made the personal data **public** and is obliged to erase such personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to **inform** the other controllers, if any, that the data subject has requested the erasure of personal data.

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Data Protection Officer

- The **designation** of a **DPO** is **mandatory** in 3 cases:
  1. The processing is carried out by a **public authority** or body, except for courts acting in their judicial capacity; or
  2. the core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require **regular and systematic monitoring** of data subjects on a **large scale**; or
  3. the core activities of the controller/processor consist of processing on **a large scale** of **special categories** of data or data relating to **criminal convictions** and offences.

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Data Protection Officer (2)

- The precise **interpretation** of the specific cases where a DPO is required by law remains **unclear**: “core activities…large scale…regular and systematic monitoring of data subjects”.

- According to the **A29 Working Party**, payroll and IT activities within a businesses are not necessarily core activities. They may be ancillary activities, thus not triggering the duty to desIgnate a DPO.

On the other hand, all organisations carry out certain activities, for example, paying their employees or having standard IT support activities. These are necessary support functions for the organisation’s core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity.

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Data Protection Officer (3)

- The A29 Working Party believes that the following activities involve the processing of personal data on a **large scale**:

Examples of large-scale processing include:

- processing of patient data in the regular course of business by a hospital
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in providing these services
- processing of customer data in the regular course of business by an insurance company or a bank
- processing of personal data for behavioural advertising by a search engine
- processing of data (content, traffic, location) by telephone or internet service providers

Examples that do not constitute large-scale processing include:

- processing of patient data by an individual physician
- processing of personal data relating to criminal convictions and offences by an individual lawyer

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Data Protection Officer (4)

- Examples of activities involving a regular and systematic monitoring of data subjects:

Examples: operating a telecommunications network; providing telecommunications services; email retargeting; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation, etc.

Data Protection Officer (5)

- The GDPR requires that the DPO shall be designated on the basis of professional qualities and, in particular, **expert knowledge** of data protection law and practices and the ability to fulfil the tasks assigned to the DPO by the law.

- The DPO can be **internal** or **external**.

- The DPO **cannot** hold a position within the organisation that leads them to determine the purposes and the means of the processing of personal data (**conflict of interests**).

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

THANK YOU…

Alan.rhode@taxmen.eu

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE