THE GDPR - ONE MONTH DOWN THE LINE

A summary

June 2018
10 Reasons not to fear the GDPR monster - and 1 to be absolutely terrified
10 Reasons......

One month down the line - and what do we know

1. The GDPR only applies to personal data - not data on companies = not BtB data
2. The IT solutions needed may be complex - the law is not (that) complex
3. Just know what you do, why you do it, and with whom
4. The GDPR gives you/your company the chance to clean up, get structured or get that overview of the data you store and use - and not use
5. With the GDPR - consent is not always the answer
6. Most of it you know you do - now you just have to inform others about it
7. Most of it you do already - now you just have to document it
8. Lots of ”low-hanging fruits” that will get you a long way towards being compliant
10. The update of Privacy policies has been extensive - and necessary
   The one (or two) thing to fear:
   1. The risk of being fined - obviously
   2. Bad publicity
PERSONAL DATA

NOTHING ELSE

So what is a *Personal* Data identifier?

- a name and surname - unique names and ordinary names;
- a home address;
- an email address - private + business address!
- an ID number;
- location data (for example the location data function on a mobile phone)*;
- an Internet Protocol (IP) address;
- a cookie ID*;
- the advertising identifier of your phone;
- a symbol that uniquely identifies a person
The legal requirements - short and sweet

Do the mapping

Know what you do, why you do it, and with whom. The GDPR gives you/your company the chance to clean up, get structured og get that overview of the data you store and use - and don’t use

Guiding principles:
• lawfulness, fairness, transparency, and accuracy
• purpose limitation, data minimisation, integrity, and confidentiality.
The legal requirements - short and sweet

What is your reason for processing data - think about it!

- Necessary for the performance of a contract to which the individual (whose data you are processing) is party
- Your future contracting party has given you her/his data with the purpose of entering into a contract
- You have to store data to comply with a legal obligation to which you as data controller is subject
- You have to store or process data in order to protect the vital interests of the individual (whose data you are processing) or of another natural person
- You perform a task carried out in the public interest or in the exercise of official authority vested in you
- You have a legitimate interests as a data controller or a third party has such interest - except where such interests are overridden by the interests or fundamental rights and freedoms of the individual (need to take a balanced view)

LAST BUT NOT LEAST: You have individual consent to process someone’s personal data for one or more specific purposes

You need to be able to document your reason!
Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person’s sex life or sexual orientation **PROHIBITED!!!!**

(UNLESS: consent, already public, non-profit organisation with ethnic, political religious, etc. purpose - members)

Criminal convictions and offences or related security measures **RESTRICTED/CONTROLLED BY THE AUTHORITIES**

Identification number/social security number **PUBLIC AUTHORITY, A LEGAL REQUIREMENT, CONSENT, SCIENTIFIC PURPOSE, EXCERCISE OR DEFENCE OF LEGAL CLAIM (and a few more)**

All other personal data such as: Contact details, hobbies and interests, shopping habits, socio-economic status, employment info, debt, family and friends, network info **HAVE A GOOD REASON! (OR CONSENT)**

Do not share data for marketing purposes unless you have active consent
With the GDPR - consent is not always the answer

When do you need consent to process data?

If none of the other legal requirements apply
If you want to use data for other purposes than the original purpose e.g. marketing
If you want to share (sell) data with (to) third parties
Rights of customer/data subject

The right to be informed

Provide information to your customers about:

1. What are the grounds/purpose (legal basis) for processing personal data
2. Categories of personal data processed
3. How long do you plan to store personal data
4. Do you plan to share data with others/others outside EU
5. Any automated decision making, the logic involved including the consequences thereof
6. The customer’s rights:
   1. The right to access own data
   2. The right to transfer data or have it removed
   3. The right to complaint
   4. The right to withdraw consent at any time
   5. The right to request rectification, erasure or restriction of processing of personal data
Rights of customer/data subject

The right of access

- Inform your customers in a clear and concise manner - no need to use formal language
- Reply to requests of access with in 1 month, or 2 months if complex
- Do not request a fee - unless excessive request!
- Refuse if unfounded or excessive request
- Request identification of customer or more specification if unclear request
- Inform about complaint procedures if you have grounds to refuse
Rights of customer/data subject

The exemptions

1. No obligation to inform if the customer knows already - and you can prove it
2. No obligation to inform if vital interests outweigh the interests of the data subject
3. Do not disclose information on third parties even if it is included in information you have to disclose = erase
Rights of customer/data subject

The right to be forgotten

Delete data when - (main reasons)

• Data is no longer necessary for the purposes for which they were collected or processed
  • Set up an automated system or a reminder
• Consent has been withdrawn AND there is no other legal grounds for the processing
  • Evaluate your need for consent
• Objection to the processing AND there are no overriding legitimate grounds for the processing
  • Balance your interests
• Unlawfully processing
  • Just do it - delete!
Rights of customer/data subject

Delete shared data /distributed data

• Take reasonable steps, including technical measures, to inform other data controllers with whom you have shared the data that they need to delete data due to requests from data subjects
• Take account of available technology and the cost of implementation
• Document what you do
Documentation is key
If you can do it, you can show it

• Write a privacy policy, and make it available
• Train your staff/yourself in how to comply
• Have your data information sheet ready
• Have a standard reply for access requests ready
• Have consent form/boxes to be ticked ready
• Have an organisation plan ready - who does what
• Have your breach plan ready - who does what
Security Breaches - report to authorities

Loss of data = report both loss of physical and electronic data
You will be fined - you will receive bad publicity

How to mitigate

Breaches:
1. Non-compliance with rights of data subjects
2. Security breach/loss of data or risk of loss of data

Mitigation:
1. Do what you reasonable can to mitigate consequences for data subjects
2. Inform authorities
3. Inform data subjects
4. Cooperate with the authorities
5. Document improvements to show compliance after breach
6. Consider taking out a cyber risk insurance
New EU preliminary ruling - facebook
C210/16 - old regulation but applicable principles

Ruling: The administrator (any private company) of a social network fan website and the host of the social network (facebook) has joint responsibility as data controllers.

According to Danish Data Authorities this means:
• YOU need to ensure adequate information to data subjects and consent if necessary
• YOU need to ensure a datacontroller agreement with the social network in order to agree on shared responsibilities
• YOU need to inform data subjects of the shared responsibility
• Data subjects can excercise their right of acces towards YOU, including the right to be forgotten
• Joint and several liability with social network host
NEXT: THE E-PRIVACY REGULATION

By the end of 2018......

June 2018