TRUSTED PRIVACY – ePrivacy

The new GDPR – legislative changes & solutions for online marketing

IAB Forum 2016
29/30th of November 2016, Milano

Prof. Dr. Christoph Bauer, ePrivacy GmbH
Your partner
We are an independent partner, largely present in Germany and Europe, specializing in digital data protection.

Framework
We operate within the framework of privacy protection, on behalf of our customers.

Advantage
We create a competitive advantage through online privacy for our customers’ digital products and services in Germany, Europe and worldwide.

Our network
We work closely with established and experienced organizations, public authorities and legislators.

Full service
We are a full-service provider, offering consulting, sealed certifications and privacy protection technologies.

References
We work with around 150 top brands around the globe.
Clients in Italy:
- nugg.ad
- Quantcast
- Rocketfuel
- DataXu
- Zeotap
- RadiumOne
- Smartclip
- Webtrekk
- x+1
- ...
ePrivacy – International Presence

International products:
- ePrivacyseal EU (on new GDPR)
- OBA certification (EU wide)
- DTSG UK Brand Safety
- ePrivacyseal CH/DE

International associations:
- IAB Europe
- Local Based Marketing Association (LBMA)
- International Association of Privacy Professionals (IAPP)

Representatives in:
- London (UK)
- Paris (FR)
- Zurich (CH)
- Brussels (BE)
- Milan (IT)
- Madrid (ES)

ePrivacy certifies in 17 countries worldwide
Headquarter in Hamburg, Germany
Facts and Figures

- Customers of ePrivacy GmbH: 150
- Awarded ePrivacyseal version EU / DE: 70
- Awarded OBA Trust Seal Certifications: 80
- Consulting projects: Big Data Privacy by Design: 10
- Other certifications: DTSG Brand Safety, Targeting Seal...: 20
- ePrivacy operates in several countries worldwide
- OBA framework determines the market standard
- Inspected mobile apps
- Cooperation with several institutions
- Involved auditors and evaluators

ePrivacy operates in 16 countries worldwide, with 250 participating companies and 950 inspected mobile apps. It has 15 partners and 20 auditors. 2011 is the year of establishment.
First fundamental change: **Start over from scratch.**

- The GDPR takes precedence over previous regulations.
- Everything we have known up to now is soon to be replaced.
- National Data Protection Act Law will be reduced to bare-bones legislation.
- A EU-wide interpretation of the new GDPR shall be achieved.
- Potential for huge fines for non-compliance – up to €20m or up to 4% of the total worldwide annual turnover, whichever is higher.
Second fundamental change: **Personal data**

- **Previously** considered personal data: Name, address, telephone number, etc.

- **Previously not** considered personal data: Cookie IDs, IP addresses, MAC addresses, etc.

- Under the **new regulation**: Any identifier is considered personal data. That means also IP addresses, cookie IDs, digital fingerprints, user IDs, etc.

- This is being contested in part. We are keeping an eye on the developments.
Third fundamental change: Privacy protection law regarding online advertising

• In and of itself, any processing of personal data requires consent.

• Art. 6(1f) GDPR: Should data processing be required in meeting the legitimate interests of the data processor while not predominating the interests of the involved individual, then the processing of personal data is permissible even without consent.

• What is a ‘legitimate interest’? Recital: direct marketing is legitimate. Does the same go for (online) advertising?

• Alignment with American law. In assessing what is legitimate, the ‘reasonable expectations’ of the party involved are to be considered. Everything that is ‘to be expected’ in that sense, is therefore legitimised.
Fourth fundamental change: In the future, **opt-out is compulsory**

Art. 21 GDPR: It is compulsory to give users the possibility to object (opt-out) to the processing of usage data.

- At the latest upon first contact, e.g. when loading a website
- Without compulsion
- For the concrete case (specific)
- In knowledge of the facts (informed, clear, plain language)
- Unambiguous expression of willingness in the form of a statement and other action.
- Also implied actions (surfing further after a pop-up) are therefore possible in the future (controversial).
- Burden of proof lies with the responsible party
- Transparency: comprehensible and easily accessible form; clear, simple language; clearly distinguishable from other text
- Withdrawal of consent: at any time and as the granting of consent
- Prohibition of coupling: The contract cannot be made dependent upon consent if data are not necessary for processing it.
Fourth fundamental change: In the future, **opt-out is compulsory**

**Example: Certification of IAB Europe OBA Framework**

In April 2011, the European associations IAB and EASA adopted a voluntary commitment for Online Behavioral Advertising – the IAB Europe OBA Framework. More than 250 companies in online profiling, targeting, user profiling and ad networks have signed the contract to date, obliging themselves in the interest of their customers and demonstrating it with the EDAA Trust Seal.

**Compliance with OBA Framework**

The IAB EDAA Framework contains 6 main points:

- Notice and transparency
- User choice over OBA
- Cookies preference management
- Exclusion of sensitive segmentation
- Legibility of OBA for users
- Process for answering user complaints
The new GDPR – legislative changes & solutions for online marketing

Fourth fundamental change: In the future, opt-out is compulsory

Example: Certification of IAB Europe OBA Framework
The new GDPR – legislative changes & solutions for online marketing

What else is mainly important for online marketing / use of data?

• Privacy impact assessment (PIA) for privacy protection (Art. 35 GDPR)
• Data protection by design/by default (Art. 25 GDPR)
• Privacy protection officer (Art. 37 GDPR)
• One-stop shop (Art 56, 1 GDPR)
• Anonymization of Data
Privacy impact assessments (PIA)

Art. 35(1):

„Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. [...]”

• so-called risk-based approach of the GDPR

• greater personal responsibility on the part of companies
Privacy impact assessments (PIA)

Art. 35(3):

“A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

a) systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;”

• In online marketing legal effects are quite seldom, e.g. the following models have legal effects:
  • Online awarding of (micro)credit based on a profile
  • Dynamic pricing, etc.

• If you don’t do that, online marketing does not have legal effects
Privacy impact assessments (PIA)

Art. 35(4):

“The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. [...]”

Art. 35(5):

“The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. [...]”

This will probably be decisive in practice!
Data Protection by Design / by Default

Art. 25(1):

“Taking into account the state of the art, [...] the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, [...] in order to meet the requirements of this Regulation and protect the rights of data subjects.”

Be compliant right from the start of your product – implement

- Pseudonymization
- Anonymization
- Opt-in/Opt-out
Data Protection by Design / by Default

Art. 25(2):

“The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.”

Example: The Opt-in box shall not be activated when the user visits a website.
The new GDPR – legislative changes & solutions for online marketing

Data protection officer (DPO)

- Embedded in existing German law, new for Italian companies

- In the future, engaging a data protection officer (DPO) is required whenever ‘[...] the core activities of the controller or the 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;” (Art. 37 (1b))

- A privacy protection officer must have specialized knowledge
- Can be engaged either internally or externally
- Tasks: Compliance and cooperation with authorities

- Necessary formats and tools are available (e.g. from www.ePrivacy.eu)
The new GDPR – legislative changes & solutions for online marketing

‘One-stop shop’

• Art. 56(1) GDPR: Oversight authority at the head office (Art. 4 No. 16 GDPR) or the individual branch office is the responsible leading oversight authority for cross-border matters.

• The leading oversight authority is the sole point of contact to the responsible party with regard to cross-border matters.

• If multiple authorities are involved, the other authorities are informed of planned decisions and can file an objection with the authority.

• In case of disagreement among the authorities, the European Privacy Commission shall decide as necessary (‘coherence mechanism’).
Discussion over anonymous data is not over

- The new Article 4 GDPR seems to imply that online identifiers are supposed to be classified as personal data. However recitals 26 and 30 suggest that not every online identifier is automatically to be classified as personal data:
  - Recital 26: „... The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous … “
  - Recital 30: „Natural persons may be associated with online identifiers … may be used to create profiles of the natural persons and identify them.“

- We have already discussed this with German data protection authorities who acknowledge the existence of anonymous data
- However, it is still unclear when exactly data is anonymous – this needs to be evaluated in detail, as there is no clear guidance in the law.

- As long as an online identifier is anonymous, the GDPR does not apply!
Discussion over anonymous data is not over

As a consequence, the online marketing industry is interested in finding ways to generate and use anonymous data.

Examples:
Hashing of email addresses

```
dff8869f11fd07218bfff6b5fc3ce3787c8f047
```

Deletion of the last octet in IP addresses

```
51.62.120.89 becomes 51.62.120.0
```

SHA
The new GDPR – legislative changes & solutions for online marketing

Requirements based on the new data protection law for use of data in online marketing

Short summary

- Existing online identifiers can still be used if “legitimate interest” can be proved
- Implement transparent information to users and implement opt-out of data use - adjust data protection declaration
- Implement privacy impact assessments (PIA) and principles of data protection by design/by default when new technology/processes are used
- Install a data protection officer (internal or external)
- Anonymous data still can be used and is not covered by GDPR. Anonymous data needs to be anonymized by clear and secure processes
- Implementation of EDAA/IAB OBA framework assures compliance of targeted advertising with new data protection law
- Full certification based on new data protection law recommended for technology companies and services (already provided by ePrivacyseal)
Case Study:  ▲ zeotap  Determium™ Audience

Leveraging privacy as a competitive advantage to win data partners

**Background:** zeotap is a global data company that activates and monetizes de-identified audience data from mobile network operators to radically optimize audience measurement and targeting on mobile devices.

**Challenge:** Mobile network operators are subject to extremely strict data privacy regulations, which can differ a lot between countries.

**Solution:** To prove the compliance with strict EU data privacy guidelines and the soon to come GDPR, zeotap certified it’s audience targeting product Determium™ Audience with the ePrivacyseal EU and the GDPR Ready addendum.

**Benefits:** Due to zeotap’s privacy-by-design technology and the ePrivacy certifications, they where able to win mobile network operators globally as data partners.
The new GDPR – legislative changes & solutions for online marketing

Do you have any questions or require further information?

• For more information please look at articles published by ePrivacy and iab Germany (BVDW), for example
  • https://www.exchangewire.com/blog/2016/05/24/gdpr-whats-relevant-for-the-use-of-cookies-identifiers-in-online-marketing/
  • https://www.exchangewire.com/blog/2016/08/24/will-still-anonymous-data-online-marketing-gdr/

• ePrivacy is happy to answer your questions – please contact us over info@eprivacy.eu or over my personal email address:

Prof. Dr. Christoph Bauer
CEO
c.bauer@eprivacy.eu

Mille grazie dell’attenzione.