

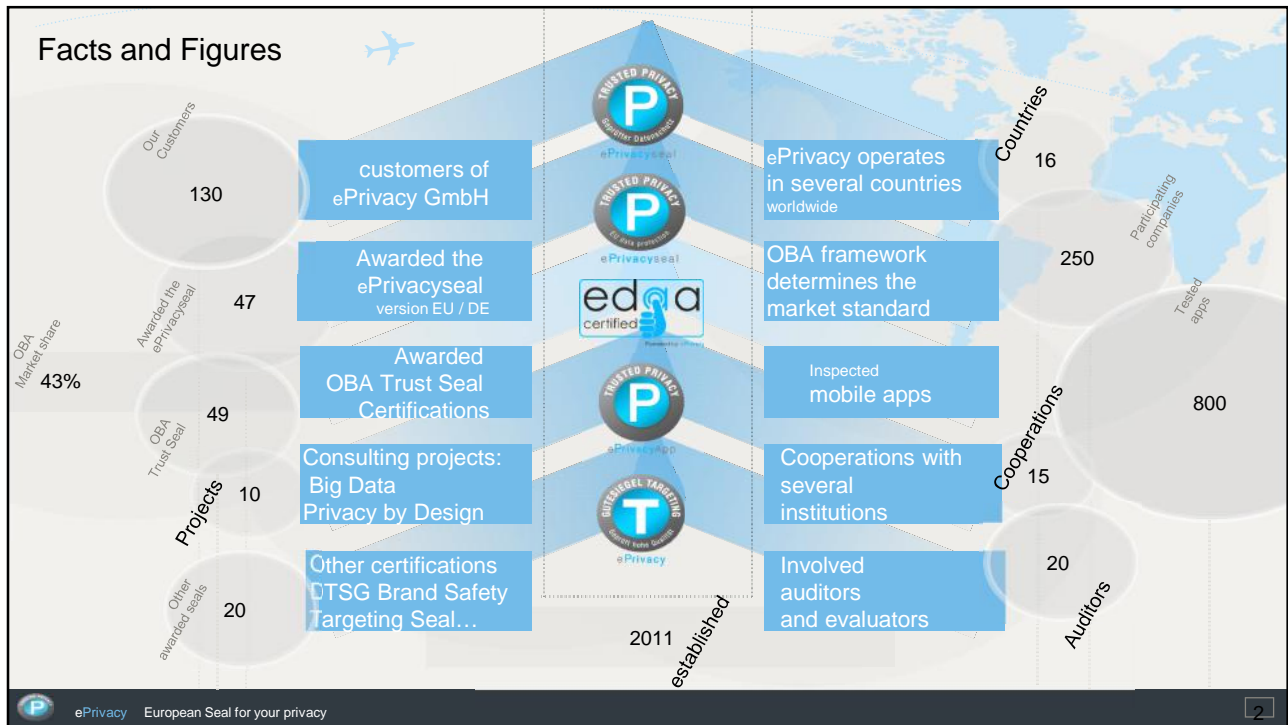


TRUSTED PRIVACY

GDPR overview & implications for the digital marketing industry

Prof. Dr. Christoph Bauer
ePrivacy GmbH

EDAA Summit 2016
Brussels, 1 March 2016



References

COMMERZBANK semasio zanox. SONIC HEALTHCARE MATTERS ADEX

ePrivacy European Seal for your privacy 3

EU General Data Protection Regulation – GDPR

important changes I – first analysis

1 Personal Data

- ▶ New definition - not only: name, address, email etc.
- ▶ Personal data now also includes: **all online identifiers like ID number, location data, cookie ID, IDFA, Advertiser ID etc. – THIS IS A FUNDAMENTAL CHANGE !**
- ▶ Permission for use of personal data needed via consent or other legitimation by law
- ▶ Pseudonymisation is introduced as a concept, where original data can only be read having a key to de-pseudonymise data. But: pseudonymised data is still treated as personal data
- ▶ Sensitive data & special personal data have more protection
- ▶ **Protection of Personal Data** with adequate “Technical and Organisational Measures“ (TOMs) is necessary

2 New Rights for Data Subjects

- ▶ Right of Information & principle of transparency (more rights)
- ▶ Right of Data erasure
- ▶ Right of **Data portability**
- ▶ Right of Data access
- ▶ Principle of Data use according to intent
- ▶ Principle of Fair use of data
- ▶ Principle of Publication of data losses (**within 72 hours**)

EU General Data Protection Regulation – GDPR

important changes II – first analysis

3

Impact on Direct Marketing / Online Marketing

see also <https://www.eprivacy.eu/aktuelles/news/>

- ▶ Consent: new definition of “informed and unambiguous consent”, not necessary “explicit”, but needs to be “informed, freely given, refusable” etc. This is a new concept, so that implied consent is also possible
- ▶ Permission for use of personal data: direct marketing is an interest of involved companies which users can „reasonably expect“ and as such is a „legitimate interest“ (Art 6(1)f). In short: It will also remain the case in the future that most of the business models in place in the online industry will not require data subjects to give their consent to the use of their data provided they stay within the bounds of their users’ “reasonable expectations”
- ▶ Websites: all providers need to inform about use of data and offer an optout for the users of the website
- ▶ Tracking: an optout for users needs to be offered
- ▶ Anonymization of data is still possible and then GDPR is not relevant, but personal data has a very large scope (see above)

4

Further Rules / Effectiveness of GDPR

- ▶ **Data Protection Impact Assessment (DPIA)** to check impact of new technologies /products on personal data and rights of data subjects has to be conducted **before implementation**
- ▶ Data Protection Officer has to be installed, if controller regularly and systematically monitors data subjects
- ▶ **Controller** shall implement internal policies and measures to follow principles „data protection by design“ and Data protection by default“
- ▶ **Companies outside of the EU** will be bound to the GDPR as well
- ▶ **Very high penalties** for misuse of personal data (up to 4% of a company’s revenue / € 20 Million)
- ▶ New regulation is directly effective in 2 years and will be replacing current national / EU data protection law



ePrivacy – contact us



Prof Dr Christoph Bauer

CEO

20 years experience in the media industry, CFO and COO at Bertelsmann and AOL, CFO/COO at wunderloop. *Member of several groups* on data protection and security issues (IAB EU, BVDW, BITKOM, BvD, GDD), with a great number of publications on online behavioural targeting, privacy and data protection. *Accredited evaluator* at ULD, certified auditor ISO 27001 / data security.



+49 40 6094518-10



c.bauer@eprivacy.eu

