GDPR Compliance Overview

What is the GDPR?

The General Data Protection Regulation (GDPR) creates a "one-stop shop" approach to data protection laws across the European Economic Area (EEA) and will come into effect on May 25, 2018. The GDPR, which will replace the current EU Data Protection Directive as the overarching data privacy framework, enhances the protection of EU residents' personal data and increases the obligations of organizations regarding the collection and processing of personal data. The full text of the GDPR can be found here.

Who does the GDPR apply to?

The GDPR applies to any entities, located anywhere in the world, that control or process the personal data of EU residents. Specifically, the GDPR applies to entities that:

- Geolocation (GPS-based or IP-based)
- Advertiser ID (IDFA/Google Ad ID)
- Internet Protocol Address (IP)
- Any other "online identifier" (e.g. device IDs, user names, etc.)

What is personal data?

"Personal data" means data of an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier. The broad scope of personal data, therefore, also includes IP addresses, device IDs, and advertising IDs.

What GDPR compliance steps should companies take, and what are some key concerns?

Project Scoping and Planning

- Identify all categories of personal data
- Create data map
- Determine if personal data transferred outside of the EEA
  - Ensure proper data transfer mechanism
- Conduct a data protection impact assessment (DPIA) for new products and features

Lawfulness of Processing

- Confirm legal basis for processing personal data
  - Legal bases include: consent, legitimate interests, legal compliance, performance of a contract with a data subject, protecting vital interests of a data subject, and processing in the public interest

- If relying on consent to process personal data:
  - Consent should be given by a "clear affirmative act establishing a freely given, specific, informed, and unambiguous indication"
  - Valid consent includes the end-user "Ticking a box" when visiting a website or choosing technical settings; "Silence, pre-ticked boxes or inactivity" are insufficient

Data Processing Documentation

- Maintain internal records about data processing activities to meet record-keeping and accountability requirement
  - Documentation must include: details regarding the types, uses, and disclosures of personal data collected

- Only collect personal data to the extent necessary for the activity or service; ensure accuracy of personal data; destroy or anonymize personal data when no longer needed

Individual Rights

- Guaranteed and applicable individual rights include: access, rectification, erasure, restrict processing, object, data portability, and rights relating to automated individual decision-making and profiling

Notice Remediation

- Provide information and notice regarding privacy practices

- Update privacy policy and employee contracts, handbooks, and other human resources related policies to inform EU data subjects of their individual rights under the GDPR

Vendor Management

- Implement checks into procurement process to ensure vendors are compliant with the GDPR

- Impose contractual provisions on vendors to properly allocate responsibility and risk

Security

- Implement (a) internal processes for regular, risk-based security gap analysis and remediation and (b) appropriate safeguards such as encryption, pseudonymisation, business continuity and disaster recovery procedures, and incident/breach response plans

- Ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services

DPO

- If required, appoint a Data Protection Officer (DPO) to oversee compliance with the GDPR
- DPO must act independently and possess data privacy expertise

Administrative Fines

- Fines of up to the greater of 20,000,000 EUR or 4% of annual, worldwide turnover, depending on the type of violation and mitigating factors
- Individual data subjects can sue for compensation for material or immaterial damage

Privacy Shield Certification and Other Cross-Border Data Transfer Mechanisms

- For U.S.-based companies, obtain Privacy Shield certification to enable the transfer of EU residents' personal data to the U.S.
- Other cross-border data transfer mechanisms include Binding Corporate Rules (BCRs) and Standard Contractual Clauses

What Compliance Steps Is Smaato Taking?

- As the May 25, 2018 deadline for compliance with the GDPR approaches, Smaato is evaluating any additional requirements imposed by the GDPR. We continue to implement and update our processes and polices as necessary to comply with the GDPR, and we are tracking industry developments and best practices
- Smaato has certified with the Privacy Shield as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from the European Union member countries and Switzerland. Smaato certifies that it adheres to the Privacy Shield Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. See our Privacy Shield certification and Privacy Policy for more information

If you have further questions or concerns, please contact your account manager or send an email to privacy@smaato.com.

San Francisco
240 Stockton St
10th Floor
San Francisco, CA 94108
T: +1 (650) 286 1198

New York
Empire State Building
350 Fifth Avenue, Suite 4210
New York, NY 10118
T: +1 (646) 650 5030

Hamburg
Valentinskamp 70
Emporio 19th Floor
20355 Hamburg
T: +49 (40) 3480 9490

Singapore
12 Marina Boulevard, #35-01
Marina Bay Financial Centre Tower 3
Singapore 018982
T: +65 6336 6815

Shanghai
1018 Changning Road
21F Cloud Nine Plaza, Changning District
Shanghai, China 200042
T: +86 21 6263 0446

www.smaato.com