
Laura Jehl, Partner (Washington DC), BakerHostetler
Melinda McLellan, Partner (New York), BakerHostetler
Jaime Petenko, Counsel (Philadelphia), BakerHostetler
GDPR Snapshot

• Became effective May 25, 2018
• Applies to organizations that:
  – Are “established” in the EU;
  – Process personal data of EU “data subjects” when offering them goods or services (whether or not for payment); or
  – Monitor behavior occurring in the EU.
• Key terms:
  – “Personal data”
  – “Processing”
  – “Controller” and “Processor”
• Max fine: greater of €20 million or 4% of worldwide annual turnover
Now What? Ongoing Challenges . . .

- **Employee Training**
  - Training as key to compliance

- **Data Protection Impact Assessments**
  - When is a DPIA required?
  - When to conduct DPIAs?
  - Who in the organization conducts DPIAs?

- **Transactional Compliance**
  - Transaction considerations
  - Diligence

- **Updates from Data Protection Authorities**
  - Guidance & complaints
  - Enforcement actions and penalties

- **B2B Marketing Compliance**
  - Lawful basis for marketing
  - Notification and opt-out
CLE CODE #1

Privacy1
Employee Training

• Identify relevant personnel who need to be trained based on position and job function
• Employee training is key to GDPR compliance
• Include training as part of onboarding
• Customize training to organization and employee position
Data Protection Impact Assessments (DPIAs)

• “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.” - Article 35 (emphasis added)

• When is a DPIA required?
  – Systematic and extensive profiling with significant effects
  – Large scale use of sensitive data
  – Systematic public monitoring on a large scale
DPIA Blacklists & Whitelists

• Article 29 Working Party guidelines include criteria which may indicate likely high risk processing

• **Blacklists**: Regulators *shall establish and make public* a list of the kind of processing operations that always requires a DPIA (Article 35(4))
  - Belgium, Germany, Ireland, Poland, United Kingdom

• **Whitelists**: Regulators *may establish and make public* a list of processing that does not require a DPIA (Article 35(5))
  - Austria, Belgium
DPIA Blacklists & Whitelists cont.

• **Required to conduct DPIAs**
  – Examples of common “blacklist” activities
    ▪ Processing involves the use of biometric data to uniquely identify individuals
    ▪ Large-scale profiling
  – Examples of unique “blacklist” activities
    ▪ *Poland*: IT products for individual use involving purely personal or household activities (such as e-readers with note taking functions)
    ▪ *Germany*: Anonymization of sensitive personal data (*e.g.*, health data), for example, by an insurance company that wants to use the anonymized data for its own purposes or share it with a third party

• **Not required to conduct DPIAs**
  – *Austria*: Processing personal data for payroll administration and complying with legal requirements concerning recordkeeping or reporting (may include “special categories” where permitted by law)
  – *Belgium*: Processing exclusively for legally required personnel administration purposes (so long as processing does not involve, for example, health data, special categories or criminal records)
DPIA Considerations

• Are there exceptions to carrying out a DPIA?
  – Legal obligation or public task
  – Already conducted a substantially similar DPIA
  – Whitelist

• Who in the organization conducts DPIAs?

• When to conduct DPIAs?

• Will DPIAs need to be revisited?

• When to consult a regulator?
Transactional Compliance (M&A)

- Involve the data privacy team early in the transaction
  - Identify whether target is subject to GDPR
  - Determine materiality
- Valuation
  - Level of target’s compliance can materially impact value
  - Indemnities
- Post-closing considerations
  - Impact on compliance posture
  - Alter purpose(s) for processing?
  - New privacy notices?
  - New consent?
Transactional Compliance (Diligence)

• Need lawful basis to share and receive data
  – Notification challenges
• Minimize the personal data shared
• Implement safeguards
  – NDAs
  – Keep personal data in EEA or implement transfer mechanisms
• Key diligence requests:
  – Policies & procedures
  – Transfers outside EEA
  – IT security
  – Complaints & breaches
  – Audits & investigations
Guidance & Complaints

- Member States are continuing to issue guidance and to pass legislation implementing GDPR
  - Member State derogations

- Number of complaints varies across EU
  - May 25, 2018: Complaints filed against Facebook, Google, WhatsApp & Instagram
  - September 2018: Brave filed complaint against Google & digital advertising companies
  - Number of high profile data breaches
  - EDPB investigating 100 cross-border complaints (as of August)
Enforcement & Penalties

- Regulators conducting audits and investigations and issuing cease processing orders; no fines yet issued
  - *France*: Formal warnings issued
  - *Germany*: Investigations into GDPR compliance; cease processing order issued
  - *Netherlands*: Investigations into GDPR compliance
  - *US*: Shareholder lawsuits filed
B2B Marketing Compliance

• Business contact information is personal data
  – Exception: Sole traders and proprietorships

• Lawful basis
  – Consent
  – Legitimate interests
    ▪ Would contact reasonably expect the communication?
    ▪ Notification and opt-out still required

• ePrivacy Directive / ePrivacy Regulation
CLE CODE #2

Privacy2
Join us for the next discussion on GDPR:
November 1, 2018
1pm – 2pm ET
10am – 11am PT

Up Next:
• California Consumer Privacy Act (CCPA)
  • How does GDPR compliance intersect with CCPA?
• Reporting Personal Data Breaches
  • Initial considerations (investigations, privilege issues, DPAs with vendors)
  • Notifying regulators
  • Notifying data subjects

Have a suggestion for a topic? Email: Lshovlowsky@bakerlaw.com
Question & Answer

Laura Jehl
T +1.202.861.1588
ljehl@bakerlaw.com

Melinda McLellan
T +1.212.589.4679
mmclellan@bakerlaw.com

Jaime Petenko
T +1.215.564.2409
jpetenko@bakerlaw.com