The impact of the GDPR on FinTech

Tanguy Van Overstraeten

FinTech and the Future of Retail Banking
Colloquium National Bank of Belgium
9 December 2016
The impact of the GDPR on FinTech

**Agenda**

1. Setting the legal scene
2. The fundamentals remains
3. Key rules likely to impact FinTech
4. Concluding remarks
Setting the legal scene
Why relevant to FinTech?

Scope of application of DP rules:

Processing of Personal Data

- Any operation performed on personal data (broad list of examples covering every use of personal data)
- Any information related to an identified or identifiable individual

> e.g.: contact details and ID card, account and credit card numbers, biometrics, cookies, location data, transactions, etc.
Data protection: today

Charter of Fundamental Rights
Art. 7 (privacy) and Art. 8 (data protection)

The Data Protection Directive 95/46/EC
National implementation required
Belgium: Privacy Act 8.12.1992

ePrivacy Directive 2002/58/EC
National implementation required
Belgium: various legislations
GDPR: as from 25 May 2018

Charter of Fundamental Rights
Art. 7 (privacy) and Art. 8 (data protection)

The General Data Protection Regulation
Applies directly in Belgium
+ limited national implementation

ePrivacy Directive 2002/58/EC
Consultation in progress
⇒ alignment with GDPR
New sanctions

Combination of increased enforceability and higher administrative fines

Boardroom issue

Fines up to the greater of:
• €20 million or
• 4% annual worldwide turnover

Turnover on “undertaking” basis in principle group turnover

> Private enforcement (civil damages, collective redress = “class actions”)

> Other regulatory sanctions:

- Warning and reprimand
- Order to comply with data subjects’ request
- Order to bring processing into compliance
- Order to inform data subjects of data breach
- Temporary or permanent ban on processing
- Order to rectify, restrict or erase data
- Ability to withdraw certification
- Administrative fines
- Suspension of data flows outside the EEA
The fundamentals remain
GDPR - Fundamental principles remain…

- Data Controller
- Data Processor

Personal Data
- Sensitive Personal Data

Stronger liability for processors
- Genetic and biometric data added
- Stronger data minimisation and accountability obligations

Processing Conditions
- Consent
- Performance of contract
- Legal obligation
- Vital interests
- Public interests
- Legitimate interests

Rules for consent tightened
Key rules likely to impact FinTech
What will be stricter? – Consent requirements

Key legal ground: validity threshold significantly raised
→ Pure opt-in

Only usable when service is truly optional

freely given, specific, informed and unambiguous

clear affirmative action (no pre-ticked boxes)

be recorded (proof)

when in writing, be clearly distinguished from other matters

be authorised by a parent if given by a child (<16) for online services

...and it can be withdrawn at any time
What will be stricter? – Transparency

In clear and plain language, accessible and concise + new content requirements

→ Need to update existing privacy notices
→ Layering approach

**Directive 95/46**

1. *details re. data controller*
2. *purpose and legal basis of processing*
3. *recipients (or categories of recipients)*
4. *rights of access and correction*

**GDPR**

- details of representative and DPO
- details of ex-EEA transfer with details of safeguards (SCC/BCR)
- data storage period
- use of automated decision-making or profiling
- details of legitimate interests, when applicable
- where consent is relied on, the right to withdraw consent
- right to complain to a DPA
- right to object to processing
- right to data portability

Layering approach
What will be stricter? – Data processing agreement

Reliance on service providers (e.g. SaaS, PaaS and IaaS)
Processors directly regulated under the GDPR
⇒ With need to review their contracts and add new requirements

Directive 95/46

1. **only process on controller’s instructions unless required to the contrary by EU law**
2. **take appropriate security measures**
3. **liability allocation**

GDPR

- details of subject matter, duration, nature & purpose of processing + types of data
- inform controller if its instructions breach law
- specific/general consent for sub-processing
- assist controller when data subjects exercise rights
- ensure personnel accessing data are subject to confidentiality
- assist controller with data security and privacy impact assessments
-delete or return personal data on termination
- provide information on compliance and submit to audits
- notify controller of personal data breaches
What will be new? – Accountability

Controller and processor

Obligation to keep record and demonstrate compliance
⇔ Notification to DPA abolished

Risk-based approach

Is processing “high risk”?  Need to conduct Privacy Impact Assessment  Consult DPA if there would be high risk in the absence of mitigating measures
What will be new? – Privacy by design/default

Privacy by Design

Ensure privacy is taken into consideration before processing personal data

Privacy by Default

The default setting must be set for the highest protection of data subjects

Currently best practice, mandatory under the GDPR
What will be new? – Data breach notification

Controller + processor

Breach

Obligation to keep data secure

Notify the DPA

- When “risk” for data subjects
- Within 72 hours unless justified

Notify data subjects

- When “high risk”
- “Without undue delay”
What will be new? – New rights for data subjects

- **Right to be forgotten**
  Obligation to erase data in certain circumstances (e.g. consent withdrawn), with exceptions (e.g. for legal claims)

- **Data portability**
  Obligation to transfer data subjects’ information from one provider to the other (similar to mobile number)

**Other relevant rights?**
- Access and rectification
- Restrictions and objection (e.g. direct marketing)
- Right in relation to automated decision-making (a.k.a. profiling)
What about Security?

Legal duty to avoid unlawful processing ➔ appropriate level of security

> Risks
  > Accidental/unauthorised destruction, modification, leak or access

> Means
  > Technical measures (e.g. firewalls, anti-virus, encryption)
  > Organisational measures (e.g. training, NDA)

> Criteria
  > Nature of data
  > State of the art
  > Implementation cost
What about data transfers?

**GDPR**

Principle = prohibition of transfers outside the EU (EEA)

> **But**

**Adequacy** (white listed countries incl. US Privacy Shield)

**Derogations** (e.g. consent, legitimate interest)

**Safeguards:**
- Standard clauses
- BCR
- Bespoke clauses
- Certificate / code
Concluding remark
Concluding remark – Key messages

- Will impact FinTech
- Goal is to strengthen trust
- 18 months to prepare!
- Use the opportunity (branding)
Tanguy Van Overstraeten
Partner – Global Head of Privacy & Data Protection
tvanover@linklaters.com
+32 (0)2 501 9405 - +32 (0)478 401569