Privacy Is Fundamental, Right?

CEELI Institute
February 26, 2021

Diletta De Cicco
Associate (Brussels)
ddecicco@steptoe.com
+32 2 626-1526
1. Data’s Value in the Digital World
2. The EU Legal Framework for the Protection Of Personal Data
3. The General Data Protection Regulation
4. Cases’ Discussion
5. Conclusion
1. Data’s Value in the Digital World
The world’s most valuable resource is no longer oil, but data.

The Economist - May 2017
Data is the Head and Tail of Our Society

Data at the heart of our right to privacy

Data at the heart of innovation
Data at the Heart of Our Right to Privacy

• Consumers routinely provide their data to get access to services (payment services, shipping services, health services, e-commerce services)

• What types of data?

**Personal Data**: data that are able to identify an individual, directly or indirectly (e.g., names, email addresses, telephone numbers, credit card details)

**Non-Personal Data**: data that cannot be used to identify a person (e.g., numbers of visits on a website, aggregate data)

Agreement on the free flow of non-personal data: “Data is the backbone of today’s digital economy. The European data economy can become a powerful driver for growth, create new jobs and open up new business models and innovation opportunities. With this agreement we are one step closer to completing the Digital Single Market”

Commissioner for Digital Economy and Society, Mariya Gabriel
2. The EU Legal Framework for the Protection of Personal Data
Convention 108+

• Convention for the protection of individuals with regard to automatic processing of personal data

First **binding international instrument** in the field of data protection

Signed in 1981 and “**modernised**” in 2018, to align with the GDPR

It sets up **principles** and **rights** to enhance data protection

It regulates **transborder data flows** and empowers **supervisory authorities** to implement the Convention
Articles 7 and 8 of the Charter of Fundamental Rights

CHARTER OF FUNDAMENTAL RIGHTS
OF THE EUROPEAN UNION

Article 7
Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8
Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.
TREATY ON THE FUNCTIONING OF THE
EUROPEAN UNION

Article 16
(ex Article 286 TEC)

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.
Data protection rules cover different aspects:

- Provide for **definitions, scope and jurisdiction**
- Define **principles and rules for data processing** activities to be lawful
- Grant **enforceable rights** to individuals and **impose obligations** to organizations processing personal data
- Set the role and functions of **supervisory authorities and judicial remedies**
3. The General Data Protection Regulation
The GDPR was adopted on April 14, 2016, and became enforceable on May 25, 2018.

It replaces Directive 95/46/EC (the Data Protection Directive) and brings EU data protection rules in line with the digital economy.

It is a Regulation – one single set of rules, allowing for more harmonisation.

It ensures the free flow of personal data between Member States and strengthens individuals rights.
Why is it so famous?
GDPR – Key Provisions

- Extra-territorial scope
  The GDPR applies to companies located in the EU and outside the EU (when they offer goods or services to EU individuals or carry out monitoring activities of EU individuals)

- Strengthening of individuals’ rights to personal data
  Individuals have new privacy rights, such as the ‘right to be forgotten’, or the ‘right to data portability’

- High fines
  The maximum fine for an infringement of GDPR provisions is 4% of a company’s worldwide turnover or €20 million

- Data Protection Authorities (DPA)
  They are independent national authorities that are given the power to enforce GDPR and ensure its correct applications
**GDPR - Key Provisions**

- **New data loss notification obligation**: The data protection authority must be notified without undue delay and where feasible within 72 hours. The individuals affected may also have to be notified.

- **Restricted data flows**: Personal data transfers are restricted unless a legal transfer mechanism applies.

- **Data Governance Rules**: Appointing a Data Protection Officer - Conducting a Data Protection Impact Assessment - Applying Privacy by Design - Implement contractual requirements.
GDPR – Key Provisions
GDPR - Data Subjects’ Rights

- **Right of access**: Data subjects can ask for access to their processed data
- **Right to rectify**: Data subjects can ask for correction when data is inaccurate or incomplete
- **Right to be forgotten**: Data subjects can ask for the erasure of their data by the data systems (in specific circumstances)
- **Right to object**: Data subjects can object to the processing, for example if based on legitimate interest
- **Right to data portability**: Data subjects can ask for personal data to be transferred directly from one controller/processor to another
- **Right to restrict the processing**: Data subjects have the right to restrict the processing of their personal data (in specific circumstances)
GDPR - Data Subjects’ Super Powers

- Right to exercise GDPR rights
- Right to lodge a complaint with an organisation
- Right to lodge a complaint with a supervisory authority
- Right to an effective judicial remedy against an organisation
- Right to an effective judicial remedy against decisions of supervisory authorities
- Right to mandate a not-for-profit body to lodge a complaint or exercise judicial rights
- Right to obtain compensation for material and non-material damages
- Right to obtain compensation for material and non-material damages

Super Powers
GDPR - New Right to Mandate a NGO to Lodge a Complaint

Art. 80 (1)

- Possibility for consumers to mandate a NGO to lodge the complaint on his or her behalf and to exercise the right to receive compensation

Art. 80 (2)

- Member States may provide that any body, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint if it considers that the rights of a data subject have been infringed as a result of the processing
4. Cases’ Discussion
Cases’ Discussions

- **Group 1**: Data Transfers – *Schrems II*
- **Group 2**: Personal Data Breaches – *British Airways*
- **Group 3**: Transparency and Consent – *CNIL v Google*
- **Group 4**: Right of Access – *NOYB v Amazon*

“You’d be surprised at the number of disruptive participants we get at these focus groups.”
CJEU, Judgment of July 16, 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, C-311/18 (“Schrems II”)
1. Data Transfers – The Rule

The protection offered by the GDPR **travels with the data**:

- Trasnfers are prohibited, unless **legal mechanism** must cover the transfer of personal data:

  - **Adequacy decision** from the EC: A third country offers an adequate level of protection and data can be transferred without requiring additional safeguards (Art. 45)
  - **Appropriate safeguards**: SCCs, BCRs, Code of conduct, certification (Art. 46 and 47)
2. Data Transfers – The Case
The Schrems Saga

June 2013 - Snowden disclosures regarding PRISM
June 2013 - Schrems complaint to Irish DPC
June 2014 - Irish High Court referral to CJEU
October 2015 - CJEU invalidates Safe Harbor
December 2015 - Schrems complaint to Irish DPC re SCCS
July 2016 - Adoption of EU-US Privacy Shield
July 2017 - Irish Court referral to CJEU
May 2018 - GDPR entry into force
July 2020 - CJEU judgement in Schrems II
**2. Data Transfers – The Case Schrems II Decision**

**Schrems II decision:**

- Invalidated the Privacy Shield as the US does not provide an *essentially equivalent level of protection*
  - Current US Law on public authorities’ right to access data transferred from the EU does not satisfy the requirements of EU Law
- **Stated that SCCs are still valid but….**
  - Third countries *must* have a level of protection of data subjects essentially equivalent to the GDPR and the EU Charter of Fundamental Rights

Challenges and Criticisms ahead...

Application of EU data protection law beyond borders: towards judicial imperialisms and Eurocentric hypocrisy?

European justice commissioner Didier Reynders acknowledged that there was “no quick fix” for transatlantic transfers in a European Commission committee last week. “It’s a real political debate; it’s not just a technical issue.”

“The problem is there’s still no judicial redress [for EU citizens’ whose data is transferred to the US],” added Romain Robert, a senior lawyer at Noyb. “If they just make another [Privacy Shield] they’ll have a Schrems III, a Schrems IV.”
ICO, Penalty Notice, October, 16 2020, British Airways plc, COM 0783542
1. Personal Data breaches – The Rule

<table>
<thead>
<tr>
<th>Data Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>“A breach of security leading to the accidental of unlawful disclosure,</td>
</tr>
<tr>
<td>loss, alteration, unauthorized disclosure of, or access to, personal data”</td>
</tr>
</tbody>
</table>

Not all personal data breaches are cybersecurity incidents and not all cybersecurity incidents are personal data breaches

<table>
<thead>
<tr>
<th>Notification to the Data Protection Authority</th>
<th>Without undue delay and no later than 72 hours after having become aware of the breach</th>
<th>No notification is needed if the breach is unlikely to result in a risk for individuals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication to the Data Subject</td>
<td>Without undue delay</td>
<td>Only when the data breach is likely to result in a high risk for individuals</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Some exceptions apply. For instance, individual communication may be substituted by a general public communication in some cases</td>
</tr>
</tbody>
</table>
2. Personal Data Breaches – The Case
British Airways – The ICO Decision

• The ICO has fined British Airways £20 million for failing to protect personal data (including payment card details) of more than 400,000 of its customers:

  - No adequate security measures to prevent the cyber-attack
  - BA was the subject of a cyber-attack during 2018
  - The cyber-attack was not detected for more than 2 months
2. Personal Data Breaches – The Case
British Airways – The ICO Decision

ICO Commissioner

“People entrusted their personal details to BA and BA failed to take adequate measures to keep those details secure.”

“Their failure to act was unacceptable and affected hundreds of thousands of people, which may have caused some anxiety and distress as a result. That’s why we have issued BA with a £20m fine – our biggest to date.”

“When organisations take poor decisions around people’s personal data, that can have a real impact on people’s lives. The law now gives us the tools to encourage businesses to make better decisions about data, including investing in up-to-date security.”
2. Personal Data Breaches – The Case
British Airways – The Class Action

• The biggest class-action lawsuit in UK history:
  - More than 16,000 victims
  - The victims could claim £2,000 each
  - A dedicated website has been launched
    https://www.badatabreach.com/
Customer data theft

We are investigating, as a matter of urgency, the theft of customer data between 22:58 BST August 21 2018 until 21:45 BST September 5 2018 from our website, ba.com, and our mobile app.

The stolen data included personal and financial details of customers making bookings and changes on ba.com and the airline’s app. The data did not include travel or passport details.

The theft has been reported to the authorities and our website is now working normally.

What to do if you have been affected

If you believe you may have been affected because you made a booking or paid to change your booking with a credit or debit card on ba.com or the mobile app between 22:58 BST August 21 2018 until 21:45 BST September 5 2018, we recommend you contact your bank or credit card provider and follow their advice.
2. Personal Data Breaches – The Case
British Airways – The Class Action

REASONS TO CLAIM

Data security:
The security of your data is important and it is time for large companies to understand that.

Financial gain:
You could receive significant compensation if you are eligible.

We make it simple:
It takes under a minute to start your claim.

START YOUR CLAIM IN UNDER A MINUTE
The BA Data Breach Group Litigation

Explanation of the Terms and Conditions

The sign-up documents are lengthy and contain legal jargon that we are required to provide to you by law. We include below a summary of the main terms found within those documents:

1. You are signing a no-win, no-fee agreement. If we don’t win compensation for you, and you keep to the terms of the agreement, you won’t be charged a penny.

2. If you do win, we will seek to recover the majority of your legal costs from British Airways and from the compensation awarded to you subject to a cap of 35%. Legal costs mean the cost of the work we have done on your behalf (including success fee) and disbursement costs such as Barrister and Court fees.

3. In the end, no matter what, you will get at least 65% of your compensation (if you win £1,000 – then you will always keep at least £650). We think that’s fair and we hope you do too. If the case succeeds, we’ll give you a full breakdown, so you’ll understand exactly what we have charged.

4. We need you to cooperate with us. We are taking a risk in taking the case on a no-win, no-fee basis. If you fail to cooperate with us by ignoring our calls or emails, then we will no longer be able to act for you and you will have terminated the retainer. Please only sign up if you are willing to cooperate.
CNIL, Deliberation of the Restricted Committee, January 21 2019, GOOGLE LLC, SAN-2019-001
1. Transparency and Consent – The Rule

**Transparency**
Any information or communication relating to the processing of personal data should be easily accessible and easy to understand (Art. 5)

**Lawfulness of the processing**
Consent is one of the legal basis under GDPR (Art. 6)

**The right to be informed**
Specific information to be provided about how they will use their personal data (Art. 13 and 14)

**Validity of consent**
Consent must be freely given, specific, informed and unambiguous (Art. 7)
2. Transparency and Consent – The Case CNIL v Google Decision

• Backstage and Background:

- May 2018 - The CNIL received group complaints from NOYB and La Quadrature du Net
- **Decision** - In January 2019 the CNIL fined Google €50million:
  A. Essential information were excessively disseminated, not clear nor comprehensive
  B. Consent was **not informed, neither specific or unambiguous**
2. Transparency and Consent – The Case CNIL v Google Decision

A. Essential information were excessively disseminated
   • Understanding advertisement personalisation processing – How many clicks?
2. Transparency and Consent – The Case CNIL v Google Decision

B. Consent was not informed, neither specific or unambiguous:

Not clear whether the legal basis is consent or legitimate interest

User accepts all of the processing of personal data as a block, including personalised advertising
Personalised Ads – The Privacy Enemy?

Your mental health for sale

How websites about depression share data with advertisers and leak depression test results

No Body’s Business But Mine: How Menstruation Apps Are Sharing Your Data

PI undertook dynamic analysis of various menstruation apps using its own data interception environment to look at the data they share with Facebook.
Datenschutzbehörde, Complaint under article 77(1) GDPR, January, 18 2019, NOYB v Amazon Europe Core, C-16/18
1. Right of Access – The Rule

- **Right(s) of access (Art. 15):**
  - Obtain confirmation as to whether or not personal data are being processed.
  - **Access to a copy of the personal data.**
  - Obtain **information about the personal data processed**
2. Right of Access – The Case
NOYB v Amazon

1. Access Request Sent to Amazon

2. Amazon did not provide all personal data requested - provided none of the necessary information

3. A complaint has been filed with the DSB.

3. APPLICATIONS

3.1. Request to investigate and to disclose information
The Complainant requests that his complaint be investigated. In particular, the Complainant requests the supervisory authority to determine which exact personal data the Respondent holds on the Complainant (see Suspicion of Incomplete Information under 2.1. of the Complaint).

We also request that the results of this investigation are made available to us in the course of this procedure, in accordance with Article 77(2) of the GDPR and the right to access the records (§ 17 Austrian Administrative Procedure Act).

3.2. Request to find a violation
Given the formal requirement under § 24(2)(5) Austrian Data Protection Act 2018, the Complainant requests to make a finding that his rights have been violated.

3.3. Request to compel the controller to fully answer the access request
The Complainant also requests that the Respondent is compelled to fully and correctly respond to the Access Request submitted by the Complainant without further delay.

3.4. Request to impose an effective, proportionate and dissuasive fine
Finally, the Complainant requests, in accordance with Article 58(2)(i) in combination with Article 83(5) of the GDPR, the imposition of an effective, proportionate and dissuasive fine, taking into account that:
  i. the gravity of the infringement, considering that the right of access is a cornerstone for the fundamental right to personal data protection (Article 83(2)(a));
### One Right vs Multiple Objectives

<table>
<thead>
<tr>
<th>The right of access as a pivotal element in a wider “architecture of empowerment” designed to democratise control over the processing of personal data in society</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collective Dimension of EU Data Protection Law</td>
</tr>
<tr>
<td>Right of access to personal data used to pursue a variety of objectives</td>
</tr>
</tbody>
</table>
One Right vs Multiple Objectives

A. Access to overcome information asymmetries

B. Access for investigative journalism

C. Access to pursue social justice goals
5. Conclusion
Have You Got Inspired?

Data subjects super powers

- Right to exercise GDPR data protection rights
- Right to obtain compensation for material and non-material damages
- Right to mandate a not-for-profit body, to lodge a complaint or exercise their judicial rights
- Right to lodge a complaint with a supervisory authority
- Right to an effective judicial remedy against decisions of supervisory authorities
- Right to an effective judicial remedy against a controller or processor
- Right to lodge a complaint to the data controller
- Right to exercise GDPR data protection rights

www.steptoee.com
Questions!
• The material in this presentation is provided for informational purposes only and does not constitute legal or other professional advice. You should not and may not rely upon any information in this presentation without seeking the advice of a suitably qualified attorney who is familiar with your particular circumstances. Steptoe assumes no responsibility for information provided in this presentation or its accuracy or completeness and disclaims all liability in respect of such information.

• Steptoe is, unless otherwise stated, the owner of copyright of this presentation and its contents. No part of this presentation may be published, distributed, extracted, reutilized or reproduced in any material form (including photocopying or storing it in any medium by electronic means and whether or not transiently or incidentally to some other use of this publication) except if previously authorized in writing.