

Personal data processed for mobile and online payments: Priceless protection?

Prof. Dr. Gloria González Fuster

14 December 2018

Business and Law Department

University of Siena



Objective of this lecture

- Understanding the relation between EU data protection and EU support of data processing through a discussion of the overlap between the GPDR and the PSD2.

EU and data protection

- A history dating back from **1977** (wish to support of European 'informatics').
- **1995**, 'Data Protection Directive' (Directive 95/46/EC):
 - the free movement of personal data:
 - ... while protecting fundamental rights.
- **2000**, proclamation of the EU Charter of Fundamental Rights.
- **2009**, entry into force of the Lisbon Treaty.

EU and data policies

- Schengen Agreement of 1985
- Development of information exchange in the Area of Freedom, Security and Justice (AFSJ)
- The EU Cybersecurity Strategy
- Building a European data economy as part of the Digital Single Market strategy.

Illustrating the importance of data (and data protection) in binding the EU as EU...

POLITICAL DECLARATION SETTING OUT THE FRAMEWORK FOR THE FUTURE RELATIONSHIP BETWEEN THE EUROPEAN UNION AND THE UNITED KINGDOM

INTRODUCTION

1. The European Union, hereafter referred to as "the Union", and the United Kingdom of Great Britain and Northern Ireland, hereafter referred to as "the United Kingdom", ("the Parties") have agreed this political declaration on their future relationship, on the basis that Article 50(2) of the Treaty on European Union (TEU) provides for the negotiation of an agreement setting out the arrangements for the withdrawal of a departing Member State, taking account of the framework for its future relationship with the Union. In that context, this declaration accompanies the Withdrawal Agreement that has been endorsed by the Parties, subject to ratification.
2. The Union and United Kingdom are determined to work together to safeguard the rules-based international order, the rule of law and promotion of democracy, and high standards of free and fair trade and workers' rights, consumer and environmental protection, and cooperation against internal and external threats to their values and interests.
3. In that spirit, this declaration establishes the parameters of an ambitious, broad, deep and flexible partnership across trade and economic cooperation, law enforcement and criminal justice, foreign policy, security and defence and wider areas of cooperation. Where the Parties consider it to be in their mutual interest during the negotiations, the future relationship may encompass areas of cooperation beyond those described in this political declaration. This relationship will be rooted in the values and interests that the Union and the United Kingdom share. These arise from their geography, history and ideals anchored in their common European heritage. The Union and the United Kingdom agree that prosperity and security are enhanced by embracing free and fair trade, defending individual rights and the rule of law, protecting workers, consumers and the environment, and standing together against threats to rights and values from without or within.
4. The future relationship will be based on a balance of rights and obligations, taking into account the principles of each Party. This balance must ensure the autonomy of the Union's decision making and be consistent with the Union's principles, in particular with respect to the integrity of the Single Market and the Customs Union and the indivisibility of the four freedoms. It must also ensure the sovereignty of the United Kingdom and the protection of its internal market, while respecting the result of the 2016 referendum including with regard to the development of its independent trade policy and the ending of free movement of people between the Union and the United Kingdom.

PART I: INITIAL PROVISIONS

I. BASIS FOR COOPERATION

A. Core values and rights

6. The Parties agree that the future relationship should be underpinned by shared values such as the respect for and safeguarding of human rights and fundamental freedoms, democratic principles, the rule of law and support for non-proliferation. The Parties agree that these values are an essential prerequisite for the cooperation envisaged in this framework. The Parties also reaffirm their commitment to promoting effective multilateralism.
7. The future relationship should incorporate the United Kingdom's continued commitment to respect the framework of the European Convention on Human Rights (ECHR), while the Union and its Member States will remain bound by the Charter of Fundamental Rights of the European Union, which reaffirms the rights as they result in particular from the ECHR.

B. Data protection

8. In view of the importance of data flows and exchanges across the future relationship, the Parties are committed to ensuring a high level of personal data protection to facilitate such flows between them.
9. The Union's data protection rules provide for a framework allowing the European Commission to recognise a third country's data protection standards as providing an adequate level of protection, thereby facilitating transfers of personal data to that third country. On the basis of this framework, the European Commission will start the assessments with respect to the United Kingdom as soon as possible after the United Kingdom's withdrawal, endeavouring to adopt decisions by the end of 2020, if the applicable conditions are met. Noting that the United Kingdom will be establishing its own international transfer regime, the United Kingdom will in the same timeframe take steps to ensure the comparable facilitation of transfers of personal data to the Union, if the applicable conditions are met. The future relationship will not affect the Parties' autonomy over their respective personal data protection rules.
10. In this context, the Parties should also make arrangements for appropriate cooperation between regulators.

EU Charter of Fundamental Rights of the EU

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.
1. Compliance with these rules shall be subject to control by an independent authority.

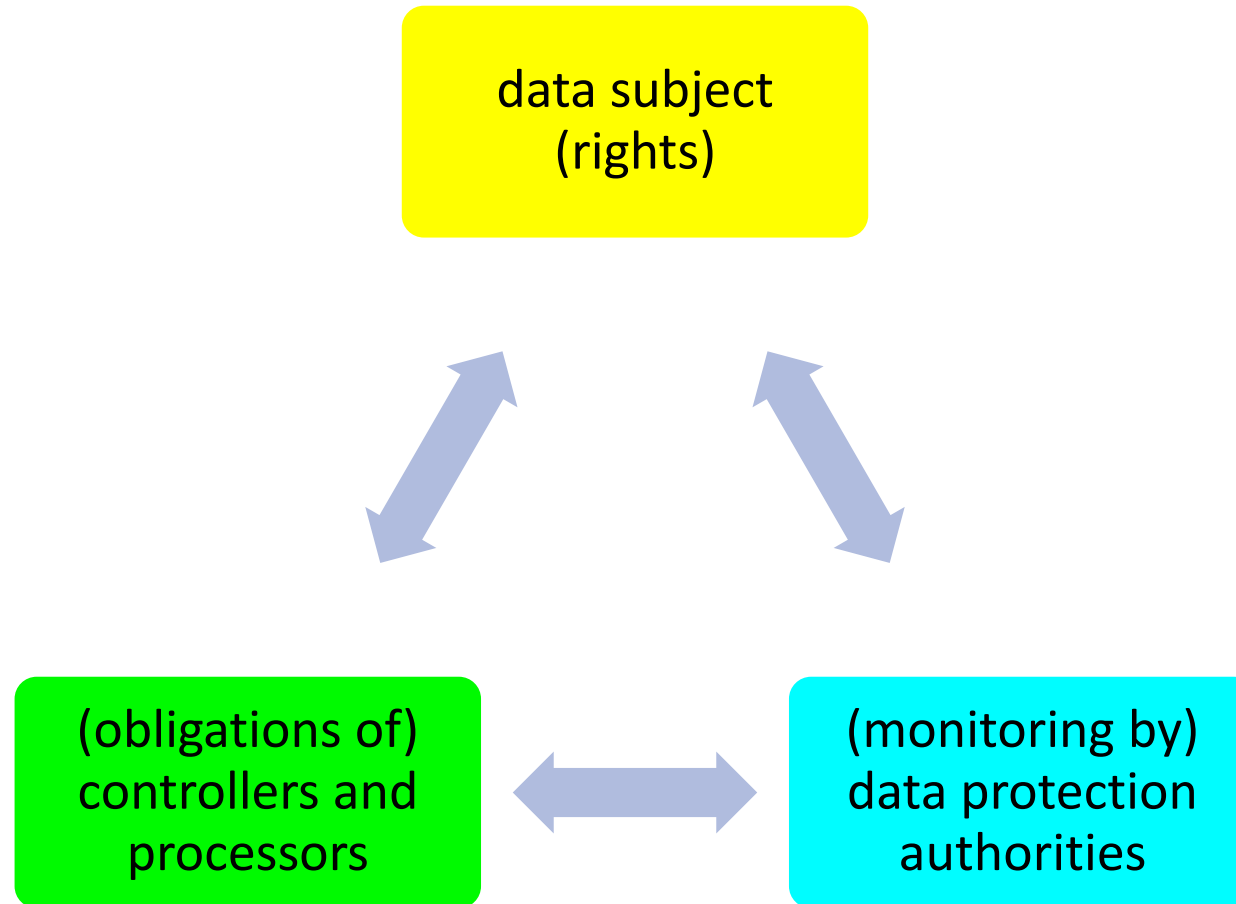
3 key points about Art. 8 of the EU Charter

- It is unprecedented at EU level.
- It is not about forbidding the processing of personal data, but about allowing it under certain conditions.
- It does not condition the processing of personal data to the consent of the individual.

Judgment of the Court of Justice of the EU of 21 December 2016
Tele2 Sverige AB v Post-och telestyrelsen, and Secretary of State
for the Home Department v Tom Watson and Others, Joined
Cases C-203/15 and C-698/15

- para. 129: *'... It should be added, finally, that Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR.'*

EU data protection



EU Charter of Fundamental Rights of the EU

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.
-
1. Compliance with these rules shall be subject to control by an independent authority.

General Data Protection Regulation (GDPR)

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- Applicable since 25 May 2018.
- Objectives:
 - Protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
 - Establishes that the free movement of personal data within the EU shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Revised Payment Services Directive (PSD2)

- Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
- Should have been implemented by 13 January 2018.
- Applies to payment services provided within the EU (Art. 2(1)).
- A key concern: to open up transactions to 'fintech' actors.

Coordination between PSD2 and GDPR

Recital (89) PSD2: **Provision of payment services by the payment services providers may entail processing of personal data.** Directive 95/46/EC of the European Parliament and of the Council, the national rules which transpose Directive 95/46/EC and Regulation (EC) No 45/2001 of the European Parliament and of the Council are **applicable to the processing of personal data for the purposes of this Directive.** In particular, where personal data is processed for the purposes of this Directive, the precise purpose should be specified, the relevant legal basis referred to, the relevant security requirements laid down in Directive 95/46/EC complied with, and the principles of necessity, proportionality, purpose limitation and proportionate data retention period respected. Also, data protection by design and data protection by default should be embedded in all data processing systems developed and used within the framework of this Directive.

In general... risk of confusion?

The case of 'sensitive' data

- GDPR:
 - Recital (10): '*... the processing of special categories of personal data (**'sensitive data'**)*'.
 - Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be [in principle] prohibited.
- PSD2:
 - Art. 4(32): '***'sensitive payment data'** means data, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data.*

PSD2

Article 94 - Data protection

1. Member States shall permit processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation and detection of payment fraud. The provision of information to individuals about the processing of personal data and the processing of such personal data and any other processing of personal data for the purposes of this Directive shall be carried out in accordance with Directive 95/46/EC, the national rules which transpose Directive 95/46/EC and with Regulation (EC) No 45/2001.
2. Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user.

GDPR - A variety of grounds for processing

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

GDPR – Definition of consent (Art. 4)

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

GDPR – Strong requirements for consent

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

GDPR – 'Compatible' further processing

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
- (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
 - (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
 - (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
 - (d) the possible consequences of the intended further processing for data subjects;
 - (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

GDPR – The ground for processing matters

Article 20

Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
 - (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
 - (b) the processing is carried out by automated means.
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Summing up... It is work in progress

- National implementation of PSD2 is ongoing.
- GDPR is being applied, the EC plans “a report” for May 2019.
- Many open questions.

Letter regarding the PSD2 Directive

Monday, 9 July 2018

EDPB



The EDPB adopted a letter on behalf of the EDPB Chair addressed to Sophie in 't Veld MEP regarding the revised Payments Services Directive (PSD2 Directive). In its reply to Sophie in 't Veld the EDPB sheds further light on 'silent party data' by Third Party Providers, the procedures with regard to giving and withdrawing consent, the Regulatory Technical Standards, the cooperation between banks and the European Commission, EDPS and WP29 and what remains to be done to close any remaining data protection gaps.

PSD2 Letter [24.35 MB](#)

English

 **DOWNLOAD**

Data protection & payments in a humanitarian context

- The 'datafication' of humanitarian aid:
 - In the context of... the datafication of everything
 - The 'evidence' / forensic turn in humanitarian aid (Eyal Weizman).
- The 'Big Datification' of humanitarian aid:
 - The Big Data humanitarian ecosystem (Linnet Taylor)
 - Big Data, (data) science and the ethics turn in (Big) data policies.



Photograph by Pierre Crom — Getty Images



Picture from <http://blog.bio-lingo.com/blogs/index.php/are-drones-the-new-telemedicine>



Meanwhile, the privacy and data protection community...

37th International Conference of Data Protection and Privacy Commissioners

Amsterdam, 27 October 2015

Resolution on Privacy and International Humanitarian Action

The 37th International Conference of Data Protection and Privacy Commissioners:

Understanding that humanitarian action aims at protecting and assisting vulnerable people in the context of armed conflicts, other situations of violence and natural disasters (together referred to as Humanitarian Crisis) often in situation of emergencies;

Considers that it covers national and international territories and is framed by national and international law, in particular international humanitarian law, international refugee law, international human rights law;

Taking into account that it brings together actors with different missions and cultures;

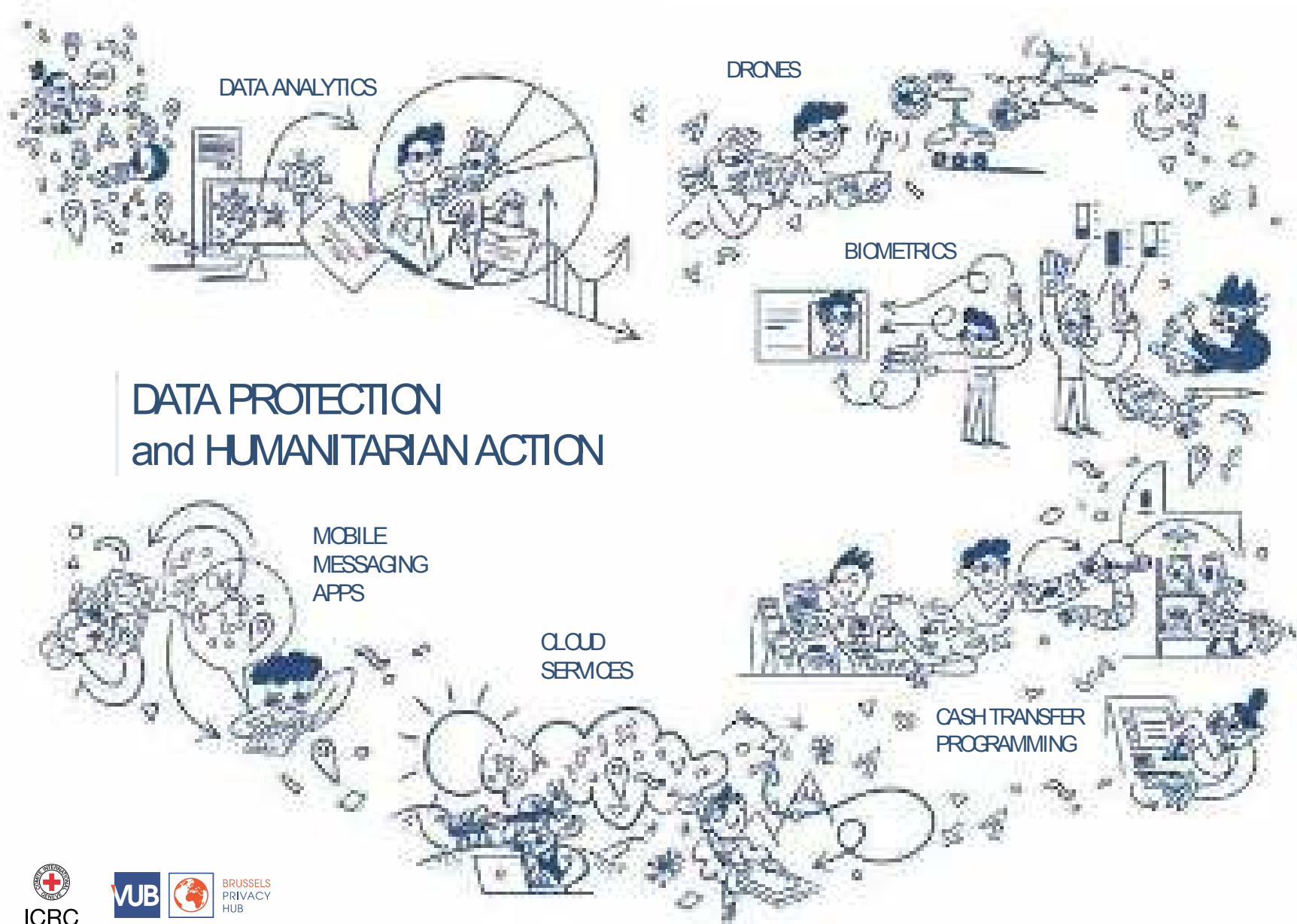
HANDBOOK ON DATA PROTECTION IN HUMANITARIAN ACTION

Co-editors: Christopher Kuner and Massimo Mucchetti



Free download

<https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action.html>



CASH TRANSFER PROGRAMMING

POSSIBLE USE

providing population with choice

supporting local markets

transparency as to how much aid reaches population

CHALLENGES

more personal data compared to aid in kind

free consent if no alternative

data retention

data sharing

incompatible further use

Increased interest in humanitarian aid through cash transfers... notably digital transfers



Data protection in humanitarian action

- Challenges:
 - a variety of actors (some enjoy privileges and immunities under international law, others not);
 - a variety of scenarios;
 - a variety of legal frameworks.
- International perspective... with a European focus?
- Thinking beyond consent... through '(local)' communities?

Concluding remarks

- The overlap between GDPR and PSD2 is ‘technically’ a challenge.
- It also demonstrates the multiplicity of interests in data access, and the difficulty (illusion) of balancing them through ‘individual consent’.
- Certainly to be continued, also in light of e-Evidence debates (cross-border access to electronic evidence in criminal investigations).

Thank you!

gloria.gonzalez.fuster@vub.be

