Legal Basis for Data Processing
Consent and Legitimate Interest under the GDPR

Benjamin Docquir
Overview: EU data protection taken to a new level

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2012</td>
<td>1st draft EU-Commission</td>
</tr>
<tr>
<td>December 2015</td>
<td>Compromise Wording by EU Parliament, Council and Commission (Trilogue Version)</td>
</tr>
<tr>
<td>27 April 2016</td>
<td>Formal Adoption</td>
</tr>
<tr>
<td>4. May 2016</td>
<td>Publication in Official Journal</td>
</tr>
<tr>
<td>24 May 2016</td>
<td>Entry into Force</td>
</tr>
<tr>
<td>25 May 2018</td>
<td>End of Transition Period</td>
</tr>
</tbody>
</table>

![Bar chart showing comparison between Directive and GDPR](chart)
GDPR – What is new?

1. Territorial Scope of the GDPR
   - Expansion of extraterritorial scope

2. Lawfulness of the data processing
   - Modifications of the requirements permitting the processing of personal data

3. Use of data processors
   - Requirements only slightly amended; increased duties of data processors

4. International transfers of data
   - Only minor changes; in the mid-term new options for international data transfers
### 5. Data Governance / Accountability

**Increased accountability requirements; new overarching burden of proof**

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Privacy Impact Assessments</td>
<td>Introduction of PIAs</td>
</tr>
<tr>
<td>b) Data Breach Notification</td>
<td>Broader notification duties</td>
</tr>
<tr>
<td>c) Data Protection Officer</td>
<td>DPO requirement across the EU (with national law specifications remaining possible)</td>
</tr>
<tr>
<td>d) Privacy by Design / Default</td>
<td>Partially new, partially stricter requirements with high relevance in practice</td>
</tr>
</tbody>
</table>

### 6. Regulators / One Stop-Shop

**Introduction of the One-Stop-Shop principle**

### 7. Fines

**Drastic increase (up to EUR 20m or 4% worldwide group revenues)**

### 8. Data Security Measures

**Minor changes, but higher relevance in practice**
Key terminology

- **Controllers**: determines the purposes and means of processing
- **Processors**: processes data on behalf of a data controller
- **Personal data**: any data which relate to an identified or identifiable natural individual (the **data subject**)
- **Processing**: virtually every conceivable operation in relation to data
- **GDPR applies to processing of personal data**: (i) wholly or partly by automated means and (ii) which form part of a filing system (= a structured set of personal data accessible according to specific criteria)
- **Sensitive data/Special categories of personal data**: (i) data revealing racial or ethnic origin, political opinions, religious or “similar” beliefs, trade union membership, (ii) data concerning health, sexual life/orientation, criminal offences/convictions, (iii) genetic/biometric data for unique identification
Legal basis – What's new?
Legal basis for data processing remain the same, only their modalities change.

- Consent
- Performance of a Contract
- Legal Obligation
- Protection of vital interest
- Performance of a task carried out in the public interest
- Legitimate interests of data controller, except where such interests are overridden by the interests or fundamental rights and freedoms of data subject

Legality Principle
Lawfulness, loyalty and transparency
Consent
When do you need consent?

• When do you need "consent" under the GDPR?
  • Consent is one of the grounds for processing personal data

• When do you need "explicit consent" under the GDPR?
  • Processing special categories of personal data (if you can't rely on any of the other lawful grounds);
  • Automated decision making (if you can't rely on either contract performance or legal obligation); and
  • Transfers of personal data to third countries (if there is no other transfer mechanism in place).
What does "consent" mean under the GDPR?

"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" [emphasis added]

Requests for consent must be:
- clearly distinguishable from other matters (i.e. no "bundled" consent)
- in an intelligible and easily accessible form
- use clear and plain language
- Contain the following info: (i) data controller; (ii) identity purposes of processing; (iii) withdrawal right

Consent can be withdrawn at any time:
- must be as easy to withdraw as to give
- data subject must be told upfront that this is possible

Other drawbacks:
- contract performance must not be conditional on consent
- clear evidence
- consent for separate processing operations = granularity
What does "explicit consent" mean under the GDPR?

• The same as under the EU's Data Protection Directive?
• The Article 29 Working Party defined "explicit consent" as:
  
  "… all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing"

• Opt-in tick box or declaratory statement
• Practically, how does this compare with "consent"?
• Is the clue in the Recitals?
• Cannot be implied from default of reaction/passivity of data subject
How to obtain consent?

- Written or oral declaration (including by electronic means);
- Ticking box
- Technical parameters of information society services

→ Any statement / behaviour clearly demonstrating acceptance of data processing

Implicit consent?
Appreciation on a case by case basis. Anyway, it has to be a sufficient externalization of consent.

E.g.: business card deposited in an urn at a trade fair for a contest; online survey.
Evidence of Consent

Data controller has to keep evidence of manifestation of data subject's will.

This implies conservation of:

- The request for consent and its annexes (e.g. Privacy Notice)
- The expression of consent (form / ticking box): to demonstrate that it was given as a result of the request for consent and at the same time
- Time when consent was given
- Name of the person consenting or his / her identifier / (?representative?)

E.g.: If consent is given during a telephone interview, it is enough for the controller to keep: notes taken by an operator, script used, time of conversation.
Inappropriate consent

When data subject cannot benefit from a genuine choice over how his/her data are being used. This is likely to be the case, for example when:

- Data controller still processes the data on a different lawful basis if consent was refused or withdrawn
  - Asking for consent is unfair and misleading → data controller can be condemned not only on the basis of GDPR but also of Book VI of BCEL relating to unfair and deceptive market practices
  - False choice and illusion of control for data subject
- Consent is a precondition of accessing the services of data controller
  - Processing necessary for the service → legal basis = processing necessary for the performance of the contract
  - Processing as a condition of services but unnecessary for the services → consent = invalid as legal basis → rather consider legitimate interest
Inappropriate consent

- Position of power of data controller over the individual – for example, an employer processing employee data
  - Clear imbalance of power
  - Fear of loosing the job
  - Compelled consent

→ Legal Basis: legitimate interest, which includes for example commercial benefit
Impact of Consent as a Legal Basis

1. Withdrawal right of data subject at anytime and withdrawal shall be as easy as giving consent
2. Impact on data subject's rights – stronger rights
   • Right to data portability
   • Right to erasure [right to be forgotten]
3. When consent is "explicit" – right for data controller to:
   • Rely on automated decisions making producing legal effects on data subject or significantly affecting him/her
   • Transfer data outside the EU, to a country with no adequate protection level (data subject needs to be prior informed about risks)
4. If data controller still process data without consent, asking for consent is misleading and inherently unfair
Key actions

- Identify data capture points (e.g. online forms, registrations, contact centres)
- Check whether opt-in/consent is really required
- What are people told about how their data will be used? (check policies, statements and notices)
- Revisit and amend any opt-in/consent forms
- Update policies, statements and notices
Practical issues where use of consent as legal basis is discutable

- Big Data Analytics
- HR and Employee Data
1. Big Data Analytics

What is Big Data?
High-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.

From the point of view of the individual concerned, Big data analytics = secondary processing

e.g. a processing that follows an initial collection of personal data (generally by another legal entity) in a very different context such as the use of social networks to publish personal information, or a commercial relationship between a consumer and a merchant.
Big Data Analytics – Choice of Legal Basis Difficulty

Difficulty regarding legal basis:

• Opaque nature of Big Data analytics makes it difficult for data subject to give a meaningful and informed consent

• ICO emphasizes that "just because people have put data onto social media without restricting access does not necessarily legitimise all further use of it. The fact that data can be viewed by all does not mean anyone is entitled to use it for any purpose or that the person who posted it has implicitly consented for further use".

• Data controller relying on consent as legal basis shall be able to demonstrate, at any time, that consent was given.

• Relying on consent means that data subject can withdraw his/her consent at any time and that data controller must then stop any data processing activity about this data subject.
Big Data Analytics – Choice of Legal Basis

As a result, though it is not unconceivable, use of consent as a legal basis for the processing of personal data for big data analytics purposes is discutable. The validity of such consent could be very easily challenged in court, with the consequence that the processing itself would be regarded as illegal.
Big Data Analytics – Purpose Limitation Difficulty

1. Big Data may imply further processing of personal data for a purpose different from that for which it was originally collected, and the data may have been supplied by a different organisation. This is because the analytics is able to mine data for new insights and find correlations between apparently disparate datasets. Big Data Companies enable the analysis of data taken from social media services (Facebook, Twitter, Pinterest, LinkedIn,… for example) for marketing and other purposes. 

\[E.g.: \text{Data about where shoppers have come from can be used to plan advertising campaigns. And data about patterns of movement in an airport can be used to set the rents for shops and restaurants.}\]

This could be seen as an infringement to the purpose limitation principle.

2. It seems difficult for data controller to benefit from the exception of "secondary processing for statistical purposes", In fact, Big Data analytics often leads to results containing personal data and used in support of measures or decisions regarding an individual.

3. **Consequence**: If data controller cannot rely on this exception → need of a different legal basis for these further processings → legitimate interest of data controller
2. HR and Employee Data

When/why does employer processes employee data?
- Control employee's achievement
- Geolocalisation of employee when outside of the office work
- HR purposes
- Protect economic, commercial and financial interests of enterprise
- Ensure proper performance of the contract

Problem Statement
- According to article 7(4) GDPR employer can not bundle the performance of the contract of employment with the agreement of the worker with the processing of his/her personal data for one or more purposes
- Consent as a legal basis can be considered as inappropriate because of the subordination position of employee.
Some scholars consider that employer can rely on employee's consent to process data and that only vitiated consent [within the meaning of civil law] would be invalid.

But this interpretation is questionable:

- **GDPR's provisions** and especially its recital 43
  
  *In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given (...) if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance".*

- and the **regulator's opinion (article 29 WP)** which emphasizes that consent will be inappropriate when given by employee because of imbalance of power
HR and Employee Data – Which Legal Basis?

Then, which legal basis?

• Processing necessary for the **performance of the contract**: processing of billing hours, salary, identity data, bank account etc.

• Processing necessary for **employer's legitimate interests**: necessity to manage employee's performance, to safeguard commercial and economic interests of employer → if well balanced and transparent information to employee, this legal basis can be justified

• **Legal obligations**: each time employer is compelled by the law to process employee data

• **Consent**: only if employer is able to demonstrate that consent was freely given (e.g.: real choice with no pressure/fear of losing the contract) or when punctual request for consent (e.g.: publication of employee picture after enterprise event)
Legitimate Interest
Processing Necessary for the Legitimate Interest

Rather than relying on data subject's consent, data controller may rely on its legitimate interests where:

"processing is necessary for the purposes of the legitimate interests pursued by the controller (...), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (...)" – art. 6(1) GDPR

Some observations:

• Concept of 'interest' = any benefit of any kind sought by an organization or any other practical concern that animates it in the exercise of its activities;

• Data processing constitute the necessary substrate of most economic, social and cultural activities;

• An organisation may have several legitimate interests that could be relevant;
Legitimate Interest – Some Observations (II)

• To meet the condition of 'legitimate interest', the processing must be "necessary" for the legitimate interest. This means that it is not enough for the processing to just be potentially interesting. It is worth noting that ICO considers that "the processing will not be considered as necessary if there is another way of meeting the legitimate interest that interferes less with people's privacy".

• This legal basis does not apply to public authority in carrying out their duties

• Data controller relying on this legal basis has to inform data subjects about its legitimate interests – art. 13(1)(d) GDPR
Is Interest Legitimate?

How to determine whether interest is legitimate? WP29 considers that "an interest can be considered as legitimate as long as the controller can pursue this interest in a way that is in accordance with data protection and other laws. In other words, a legitimate interest must be ‘acceptable under the law’".

Legitimate interest has to be:
- Lawful
- Effective
- Concrete (≠ hypothetical)

The fact that the controller has such a legitimate interest in the processing of certain data does not mean that it can necessarily rely on it as a legal ground for the processing.

Whether it can be relied on legitimate interest will depend on the outcome of the balancing test between data controller's legitimate interest and data subject's interests and fundamental rights and freedoms.
Balancing data controller's interests vs. Data subject's rights and interests

When carrying out the balancing test, four main factors will have to be taken into account:

• assessing the controller’s legitimate interest: such as commercial and societal benefits;

• impact on the data subjects: organisation will have to pay particular attention to how the processing (e.g. analytics) may affect people's privacy, to the categories of data being collected;

• provisional balance: the more organisation complies with the GDPR provisions the less likely it is going to interfere with data subject's rights and interests. But compliance might not be enough, especially in a Big Data context and organisation may have to take further steps;

• additional safeguards applied by the controller to prevent any undue impact on the data subjects: such as technical and organisational measures.
Balancing the Interests

Recital 47 provides that data controller shall take into account data subject’s expectations in order to determine whether the legitimate interest overwhelm data subject's interests. Data subject's interests and rights may, for example, prevail on data controller's interests when the data subject does not reasonably expect further processing.

Application of these principles to Big Data Analytics:

• Data controller will have to have a framework of values against which to test the proposed processing, and a method of carrying out the assessment and keeping processing under review = it takes on more responsibility

• Data controller will also need to be able to demonstrate that it complies with such balancing test when objections are raised by data subjects or regulator.

• Depending upon the context, these obligations may include a certain degree of openness and transparency about the algorithmic models used by data controller for its business operations, for instance, or other practical steps aimed at mitigating the risks and threats posed by the recourse to big data analytics.
Legitimate Interest – To Sum Up

1. Identify Legitimate Interest

2. Balance interests at issue
   + demonstrate that pursued interest justifies data processing
   + demonstrate that measures are taken to counteract data subject's risks

3. Transparently inform data subject about legitimate interests

Measures to mitigate privacy infringement risks:
- Strict limitation of processed data
- Technical and organisation measures to prevent automated decisions
- Anonymisation/pseudonymisation technics
- Aggregate data
- Strengthened transparency
- Facilitate exercise of data subject’s rights
- …
Legal basis: from data subject's consent to data controller's legitimate interest

**Consent**

- **Under Directive 95/46**
  - Apparent certainty for enterprises and more reliable
  - Consent of data subject given through acceptation on General Terms and Conditions or contract

- **Under GDPR**
  - Objectively limited: unbendable and inappropriate consent when imbalance of power
  - More demanding: request for consent = separate form and real freedom of choice
  - More uncertain: withdrawal right at any time

**Legitimate Interest**

- **Under Directive 95/46**
  - Uncertainty inherent from the exercise of interest weighting

- **Under GDPR**
  - More reliable legal basis: with appropriate balancing test + transparency measures
  - Sole appropriate response where consent is inappropriate
GDPR Principles and Secondary Processing
Principles Remain the Same but are Strengthened

Legality
- DATA Collection
- Quality
- Retention period

Purpose
- PROCESSING Consent or not? Further Use Recipients

Accountability
- Principle
- SECURITY Protection by design and by default

Proportionnality
- DATA TRANSFERS

Lawfulness
- DATA SUBJECT’S RIGHTS Stronger and new rights
Purpose Limitation and Data Minimisation Principles

Purpose Limitation Principle

Under article 5(1)(b) of the GDPR, personal data must be collected only for well defined purposes, and may not be further processed for other purposes.

4 exceptions:

• If the purpose of the secondary processing is "compatible" with the purpose of the initial collection, taking into account, notably, any link between the initial purposes and the secondary purposes, the context of the initial collection and the expectations of the individual, etc.; or
• If the secondary processing pursues "statistical purposes", provided however that in such a situation the result may not contain personal data and may not be used in support of measures or decisions regarding any individual; or
• If the individual has given his/her consent, on the understanding that such consent must be freely given and duly informed, and that it may always be withdrawn.
• (secondary purpose is based on a EU or MS law – art. 23 GDPR)
Purpose Limitation and Data Minimisation Principles

According to WP29 Guidelines, for further processing, organisation will have to consider if, and to what extent:
(i) the new purpose affects the privacy of the individuals; and
(ii) it is within their reasonable expectations that their data could be used in this way.

How to comply with this principle
• Draft a Privacy Notice which is comprehensive enough to inform data subject about the processing, its purposes, and the rights of data subjects;
• Specify the purposes according to which data are processed
• Take into account expectation of data subject for further processing and potential harm.
Purpose Limitation and Data Minimisation Principles

Data Minimisation Principle

Article 5.1c) of GDPR provides that data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

E.g. of potential difficulty: Big Data analytics tends to involve collecting and analysing as much data as possible. The issue here is not simply the amount of data collected and processed but also to determine whether it is necessary for the purposes of the processing, or excessive.

Organisation needs to be able to demonstrate, beforehand, that the data is relevant for the purposes of processing and not excessive in relation to that aim. Finding correlations afterwards, will not be an acceptable means of proving that the data processed were relevant.

How to comply with this principle?

• Define the purposes of the processing and establish what data will be relevant
• Good practice: implement good information governance and enforce retention schedules in order to prevent data storage for a longer time than necessary for its initial purposes.
Takeaways

1. **Important to identify:**
   - data capture points
   - information provided to data subject about the data processing
   - necessity of data subject's opt-in for data processing

2. **Legal Basis remain the same under GDPR / Their modalities change**

3. **Consent as a legal basis become harder to justify**

4. **Data controller can rely on other legal basis, in particular, its legitimate interests**

5. **GDPR Principles remain the same but are strengthened**
   - Purpose limitation principle
   - Data minimisation principle
   - Accountability principle
Benjamin Docquir
Partner
T +32 2 515 9336
M +32 479 38 99 25
benjamin.docquir@osborneclarke.com
Osborne Clarke is the business name for an international legal practice and its associated businesses. Full details here: osborneclarke.com/definitions