**General Data Protection Regulation (GDPR) key changes/impact specifically related to ‘consent’**

**Effective from May 2018**

Summary

1. Consent remains a lawful basis to transfer personal data under the GDPR; however, the definition of consent is significantly restricted. **Where the Data Protection Act allowed controllers to rely on implicit and “opt-out” consent in some circumstances, the GDPR requires the data subject to signal agreement by “a statement or a clear affirmative action.”**
2. The new law maintains the distinct requirements for processing “**special categories of personal data”** that were present in the Directive, but it **expands the range** of what is included in those special categories.
3. The GDPR introduces **restrictions on the ability of children to consent to data processing without parental authorization**.

Consent

Under the GDPR, consent must be “freely given, specific, informed and unambiguous” and expressed “by a statement or by a clear affirmative action.” An affirmative action signalling consent may include ticking a box on a website, “choosing technical settings for information society services,” or “another statement or conduct” that clearly indicates assent to the processing. “Silence, pre-ticked boxes or inactivity,” however, is presumed inadequate to confer consent. The GDPR removes the ability to use an “opt-out” method of consent by requiring the data subject to make a statement or clear affirmative action. **Consent must also be obtained for each distinct use of an individual’s data (you can no longer package together multiple uses).**

Gives data subjects the right to withdraw consent at any time and “it shall be as easy to withdraw consent as to give it.” Researchers must inform data subjects of the right to withdraw before consent is given. **Once consent is withdrawn, data subjects have the right to have their personal data erased and no longer used for processing.**

Where the data subject exercises her right to restrict data processing, the researcher may only continue to process the data if it obtains the data subject’s consent or if processing is necessary for a legal claim.

The data subject has the right to receive all the personal data about her in the researcher’s possession where the processing is based on her consent. In these circumstances, the required level of consent is “unambiguous” consent.

When Explicit Consent is required

The GDPR requires a higher level of consent – *“explicit” consent* – for the processing of “special categories of personal data.” [*Explicit consent - “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.”]*

These special categories relate to personal data that are “particularly sensitive in relation to fundamental rights and freedoms” and, therefore, “deserve specific protection.” They include data “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership. **The GDPR expands the definition of sensitive data to include the processing of genetic data, biometric data for the purpose uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.”** To note: photographs will qualify as biometric data only when they are processed “through a specific technical means allowing the unique identification or authentication of a natural person.”

The GDPR requires the data subject’s *explicit* consent in two other circumstances.

Researchers need to obtain explicit consent to make decisions about the data subject “based solely on automated processing, including **profiling**.” For example learning analytics – this refers to the so called ‘Big data’ and using information to predict behaviours. Inform a data subject at the time data is collected not only of the fact that profiling will occur, but as well “the logic involved” and “the envisaged consequences of such processing.” A data subject may also inquire of a controller and receive confirmation of any such processing, including profiling and its consequences, at any time. Even when profiling is otherwise lawful, a data subject has the right to object at any time and the processing must cease unless the researcher demonstrates “compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.”

Researchers also must seek explicit consent, to authorize **transfers of personal data** to countries that do not provide an adequate level of protection, if no other transfer mechanism is in place.

Restrictions on the ability of children to consent to data processing without parental authorization

**GDPR requires parental consent for processing children’s personal data. Researchers** must obtain the consent of a parent/guardian when processing the personal data of a child under the age of 16. However, EU member states can set a lower age not below 13 years.

Also,

Privacy Notices

A privacy notice that discloses the ways in which an organisation will obtain, record, hold, alter, retrieve, destroy or disclose personal information will need to be provided whenever personal data is collected i.e.

all participant documentation/web portals and must state the legal basis for the processing. The following summarises the privacy information that researchers will need to provide in their documentation to data subjects to comply with the GDPR:

* details of the purpose and legal basis i.e. consent of the processing of the personal data [The *most obvious example is that participants will have a stronger right to have their data deleted where researchers use consent as their lawful basis for processing];*
* categories of personal data processed;
* details of how their personal information is to be used;
* information about security of their data;
* information about cookies (or comparable tracking technology) used by a website [*A data subject must provide specific, informed consent to the use of cookies. However, the GDPR provides an exception where cookies are “strictly necessary for the legitimate purpose of enabling the use of a specific service requested by the subscriber or user.” It also provides that “the user’s consent to processing may be expressed by using the appropriate settings of a browser or other application.” The browser settings exception applies only if the browser’s default rejects the placement of cookies, thereby requiring the user to actively opt-in to receiving cookies.”]*
* details of the recipients of the personal data;
* right to complain;
* the period of time the personal data will be stored;
* details of any transfers of personal data outside of the European Economic Area.

Overseas Transfer of Personal Data

The GDPR largely preserves the current Data Protection Act with regard to overseas transfer of personal data. For example, prohibiting transfers of personal data outside of the EEA unless certain conditions are met (adequacy). For example, does the intended transfer involve a country which has an adequacy decision (deemed acceptable by the EU), or if based in the USA an organisation which has joined the EU-US Privacy Shield?

If you are intending to transfer personal data outside the EEA and the country has not been deemed to offer an adequate level of protection you will need to ensure that the transfer meets one of the other requirements of the GDPR, such as by use of standard contractual clauses or binding corporate rules (BCRs). Derogations (exemptions) are also permitted under limited additional circumstances. Explicit consent is one such derogation. If you know at the outset of your research that you intend to transfer personal data to another country you should inform data subjects of this and where necessary seek consent.

Further reading

* UCL Data Protection/FOI webpages: <http://www.ucl.ac.uk/legal-services/guidance/dp_GDPR>
* Information Commissioner’s Office: <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/> and a 12 step guide: <https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf>
* <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr> In particular:

[**Part 1: Cybersecurity and data breach notification obligations**](https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/)
[**Part 3: Consent**](https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/)[Part 4: Cross-border data transfers](https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/)
[Part 5: Profiling](https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-5-profiling/)

[**Part 8: Pseudonymization**](https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization)