FACTSHEET

Individual's Rights in the EU GDPR and US Privacy Shield

Updated data protection legislation comes into effect in Europe in May 2018. It gives individuals new rights to better control their personal information and strengthens some of the rights that already exist. Enforcement and redress mechanisms have also been strengthened to ensure that these rights are respected. And – importantly – the definition of personal data is wider in GDPR than in the current EU legislation or the Privacy Shield, and now includes online identifiers, such as an IP address.

How do these new rights affect the US-EU Privacy Shield agreement?

Significantly, the geographical reach of the new law has been widened: organisations that target European consumers with offers of goods and services, or monitor their online behaviour will also be subject to the rules of the GDPR. **This means that US organisations that are subscribed to the Privacy Shield must respect individuals' rights as prescribed by the GDPR as this Regulation will trump the Privacy Shield**.

The 8 Rights:

1. **to information**
   GDPR: Individuals must be provided information about who is using the data and what for. The information must be concise, transparent, easily accessible, in clear and plain language, be comprehensive, and be given at the time the data is requested or obtained.
   PS: It is called 'Notice' and its requirements are less comprehensive.

2. **to access**
   GDPR: Individuals have the right to access their personal data on request and free of charge, no matter whether it is collected directly from them or obtained from a third party. If automated decision making and profiling is done, individuals have the right to request meaningful information about the logic involved and the likely consequences. Requests must be complied with within 30 days.
   PS: Access is more limited, e.g. does not include provision of information regarding the automated decision making and profiling. Organizations can charge a non-excessive fee and must respond in a reasonable timeframe.

3. **to rectify**
   GDPR: Individuals have the right to have personal data corrected if it is inaccurate or incomplete; they must be informed about third parties to whom the data has been disclosed; third parties must be informed of the correction where possible.
   PS: There is no separate rectification principle; under the access principle individuals can have the data corrected, amended or deleted where it is inaccurate or processed in violation of the Principles.

4. **to delete (or "to be forgotten")**
   GDPR: Individuals have the right to request that personal data be deleted or removed where there is no compelling reason for its continued processing. It is not an absolute right and it's subject to a number of tests and exceptions, including freedom of expression, historical or archiving reasons; there are extra requirements when the data belongs to a child.
   PS: There is no separate deletion principle; it is mentioned under access and is only possible if the data is inaccurate or processed unlawfully.

5. **to restrict processing**
   GDPR: Individuals have the right to 'block' or suppress processing of personal data in particular circumstances (e.g. processing is unlawful or the accuracy is contested). This means personal data can be stored but not further processed until the issue is resolved.
   PS: There is no ability to restrict processing.

6. **to data portability**
   GDPR: Individuals have the right to obtain and reuse their personal data for their own purposes across different services. They can move, copy or transfer their personal data from one provider to another in a "commonly used and machine-readable format." This only applies to data that they provided themselves, based on consent or a contract.
   PS: There is no principle for data portability.

7. **to object**
   GDPR: Individuals have the right to object to processing for certain purposes such as legitimate interest or exercise of official authority. This means that such processing must be stopped unless compelling legitimate grounds which override the interests of the individual can be demonstrated. Processing for direct marketing purposes, including profiling, must always be stopped when objected to.
   PS: There is no principle to object to processing for direct marketing or other purposes.

8. **to avoid automated decision making and profiling**
   GDPR: Individuals have the right not to be subject to decisions based on automated processing without any human intervention, if such a decision can cause them harm.
   PS: There is no principle in this regard.

What about consent?

GDPR: Consent is one of the 6 basis for lawful processing, and it has to be "freely given, specific, informed and unambiguous" by taking a clear affirmative action. This means there can be no assumption that consent is given (e.g an individual can tick a box on a website to give consent but a pre-ticked box cannot be used); in the case of data considered sensitive, such as political opinions or genetic or health data, consent must also be 'explicit.' Consent must be able to be withdrawn at any time, as easily as it was given.
PS: Under the principles of Notice and Choice, individuals can limit use and disclosure of their personal information, on an opt-out basis (opt-in for sensitive information) if it will be shared with third parties or used for a purpose other than that for which it was collected. There is no general consent principle.

What possibilities for redress do individuals have?

GDPR: If their rights have been infringed, individuals can lodge a complaint with the relevant data protection authority; seek judicial redress (and compensation) against either the authority or the infringing company; or mandate a competent NGO to take the case on their behalf. In some countries, collective action will also be possible.
PS: Organizations must have independent recourse mechanisms to investigate and remedy complaints. Individuals can request binding arbitration, free of charge, only if they have attempted to resolve their complaints first directly with an organization and were unsuccessful and only for non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question). There is no provision for individuals to seek judicial redress except to enforce arbitration decisions.