General Data Protection Regulation (GDPR)

Frequently Asked Questions (FAQs)

Overview

What is GDPR?

The European Union's General Data Protection Regulation (GDPR) is a data privacy regulation that replaces the Data Protection Directive 95/46/EC, effective 25 May 2018. The GDPR is directly applicable in each EU Member State and is intended to harmonize data protection requirements across the EU. It governs handling of personal data and sets out obligations for data controllers and data processors (defined below).

Whose personal data is covered by GDPR?

EU residents and anyone who has data processed (processing includes collection, access, analysis, storage, transfer, deletion) inside the EU.

What is a Data Controller?

The entity which alone or jointly with others determines the purposes and means of the processing of personal data. For UL's software solutions, our customers are the data controller.

What is a Data Processor?

The entity that processes personal data as instructed by the data controller. UL is a data processor for our customers.

What constitutes personal data and special category personal data?

Personal data is any data by itself or in conjunction with other data that can identify a living natural person.

Special category personal data – Includes the following categories of data that are considered "sensitive" under the regulation:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Data concerning health or sex life and sexual orientation
- Genetic data
- Biometric data where processed to uniquely identify a person

What are the individual rights under GDPR?

Rights of the data subject include all the following categories:

- **Right to be informed:** Data subjects have the right to be informed about how their personal data is used.
- **Right to access information:** Data subjects have the right to confirm that their data is being processed, as well as the right to access the personal data itself.
- **Right of rectification:** If personal data is inaccurate or incomplete, data subjects have the right to have their personal data corrected.
- **Right to erasure/to be forgotten:** The data subject has the right to request that personal data be

deleted/removed when it is no longer necessary for processing and where that data is not required for any other legal, regulatory, or legitimate business reason.

- **Right to restrict processing:** In some cases, data subjects have the right to block the processing of personal data. In these cases, the data may be stored, but cannot be processed.
- **Right to data portability:** Data subjects have the right to move, copy, or transfer their data to reuse it for their own purposes. The data controller is obliged to provide this information in a format easily transferable.
- **Right to object:** The data subject has the right to object to their personal data being processed for direct marketing purposes; scientific/historical research or statistical purposes, or processing based legitimate interests or the performance of a task in the public interest. For objections to processing based on legitimate interests, the processing must stop unless there are compelling legitimate grounds for the processing that override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defense of legal claims.
- **Rights in relation to automated decision making, including profiling:** Under some circumstances, individuals are protected against the risk of a potentially damaging decision made by automated means (without human intervention). If a decision is based on automated processing and produces a legal impact or other significant effect on the individual, a data subject has the right to obtain human intervention. An example of this would be an online loan application that has been through an entirely automated process and rejected. The subject of the application would have the right to ask in this case to have a human being review the data.

However, some of these rights are not absolute. For example, the right to erasure /to be forgotten cannot be executed if there is a legal or regulatory requirement to maintain this data.

Does GDPR mean that the data must reside in EU member states?

No, the GDPR does not require EU personal data to stay in the EU, nor does it place any new restrictions on transfers of personal data outside the EU. Businesses may transfer personal data to a country outside the EU based on a mechanism from which an adequate level of data protection can be guaranteed, e.g. the standard contractual clauses approved by the EU Commission ("Model Clauses"). GDPR continues to allow for transfers of personal data based on Model Clauses. A pre-signed Model Clause Agreement is available on our GDPR website for customers who transfer EU personal data to one of UL's products residing outside the EU to countersign and return to us.

Do we need to get any additional contract terms in place with UL?

Yes, if you have personal data of any European residents stored within UL's products, the GDPR requires certain contractual terms be in place. These terms are incorporated into our Master License and Service Agreement for new customers. A pre-signed GDPR Processor Terms Addendum is available on our GDPR website for existing customers to countersign and return to us.

Are UL software solutions compliant to GDPR?

Yes. We have developed functionality allowing customers to honor "right to be forgotten" requests in the software and customers can provide data subjects with access and rectification of their data within the software. We also maintain strict security processes for the protection of personal data, in accordance with ISO 27001 and/or SOC 2 Type II audit requirements.

How are "right to be forgotten" requests implemented?

The GDPR "right to be forgotten" is accomplished by customers submitting a request at Data Subject Access Request Portal.

Does UL use any third-party vendors (sub-processors)?

Yes, UL does utilize third-party vendors. These third-party vendors have been vetted for GDPR alignment. The list of current third-party vendors and their location can be found on our GDPR website. Any updates to the use of third-party vendors will be posted on our GDPR website and customers can sign up on the website to receive email notice of any changes.

How does UL manage data transfers to a third country under the GDPR?

Data transfers to third-party non-EU state vendors is limited to those vendors who have been vetted for GDPR alignment. All data transfers are executed via a secured and encrypted method.

All vendors have signed required GDPR data processor terms, including security obligations, and have signed model clause agreements.

Who is UL's supervisory authority?

UL's supervisory authority is the Office of the Data Protection Commissioner in Ireland www.dataprotection.ie

Does UL have a Data Protection Officer?

UL is not obligated to have a DPO, as UL does not or is not:

- A public authority;
- Carry out large scale systematic monitoring of individuals (for example, online behavior tracking); or
- Carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

However, UL does have a Data Privacy Director located in Dublin, Ireland. The Data Privacy Director may be contacted at 33 Westland Square, Pearse Street, Dublin 2, Ireland or gdpr@ul.com

Where can I learn more about GDPR?

See the EU Commission website: https://ec.europa.eu/info/law/law-topic/data-protection_en and www.gdprandyou.ie for more information.