Abans Global Limited

General Data Protection Regulation

(Updated in Dec 2024)

Abans Global Limited
Regd.Office: 3rd Floor, 19 Gerrard Street, London, W1D 6JG, UK ✆ +44 (0) 203 868 5803 www.abansglobal.co.uk
Abans Global Limited is Authorised and Regulated by the Financial Conduct Authority (FRN 580056) Reg in England and Wales under Company No 7225900

Table of Content

1. What is GDPR?

The General Data Protection Regulation (GDPR) is a regulation implemented across the European Union (EU) to protect individuals' privacy and personal data. However, following Brexit, the United Kingdom (UK) is no longer a part of the EU, but it still retained much of the GDPR framework. In the UK, this law is known as the UK GDPR.

The UK GDPR applies to organizations processing personal data in the UK, regardless of where the organization itself is based. The law is designed to safeguard individuals' personal data and gives individuals control over their own data.

The main focus of the General Data Protection Regulation (GDPR) of Abans Global Limited (AGL) is the protection of personal data and digital privacy.

2. UK GDPR and the ICO

The Information Commissioner's Office (ICO) is the UK's independent authority that oversees compliance with data protection laws. The ICO provides guidance on the application of the UK GDPR and handles complaints, investigations, and enforcement actions.

Please refer to the link - https://www.gov.uk/data-protection

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles.

The EU General Data Protection Regulation ("GDPR") comes into force across the European Union on 25th May 2018 and brings with it the most significant changes to data protection law in two decades. Founded on the fundamentals of privacy by design and a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

The UK GDPR is a version of the General Data Protection Regulation (GDPR) that was adopted by the UK following Brexit. It governs the processing of personal data in the UK, not the European Union (EU)

3. Cross-Border Data Transfers

From the UK to the EU: As of now, the EU has granted the UK an "adequacy decision", meaning personal data can flow freely from the EU to the UK without additional safeguards. This ensures that data can be transferred between the EU and UK without the need for extra-legal measures.

From the EU to the UK: Similarly, UK-based businesses can continue receiving data from the EU under the same "adequacy" decision, assuming the UK maintains the required level of data protection. This law is designed to accomplish two main things:

1. Unify the current data protection privacy laws throughout the UK, and
2. Enhance the rights of citizens of the UK to protect their personal information

4. Who the GDP applies to

The GDPR applies to any business that does one or both of the following:

- Offers products or services to citizens of the UK.
- Collects personal information from citizens of the UK.

Based on the above premise the GDPR Applies to Abans Global Limited (AGL)

5. Our Commitment

AGL ('we' or 'us' or 'our') are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection framework in place which complies with existing law and abides by the data protection principles. However, we recognize the requirement and importance of updating and expanding this program to meet the demands of the GDPR and the UK's Data Protection Bill.

AGL is dedicated to safeguarding the personal information under our responsibility and to developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation.

6. AGL Policy Statement

The Board of Directors and management of Abans Global Limited (AGL) are committed to compliance with all relevant UK and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information AGL collects and processes in accordance with the General Data Protection Regulation (GDPR).

AGL's compliance with the UK GDPR is described by this policy and applies to all of AGL's personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organization processes from any source.

This policy applies to all Employees/Staff and interested parties of AGL such as outsourced suppliers. Any breach of the GDPR will be dealt with under AGL's disciplinary policy and may

also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

All third parties working with or for AGL, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by AGL without having first entered into a data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which AGL is committed, and which gives AGL the right to audit compliance with the agreement.

AGL lists six legitimate purposes, and processing of personal data must be linked to one of these.

1. **Purpose limitation.** Processing of personal data will be limited to the legitimate purpose for which that personal data was originally collected from the data subject. This effectively forbids the processing of personal data outside of the legitimate purpose for which the personal data was collected.
2. **Data minimization.** When collecting data, only the personal data absolutely required for that purpose may be requested. This means that no data other than what is necessary can be requested, or stored. This is of significance when AGL is analyzing data. It will be important to limit the analysis of data to a set of anonymized data, or to a set of data for which consent has been obtained or there is a clear legitimate processing purpose.
3. **Accuracy.** Personal data of data subjects must always be accurate and kept up to date. This is simple and straightforward, meaning that controllers are asked to ensure that data is kept accurate, and data subjects can update their data when required.
4. **Integrity and confidentiality.** Personal data must be processed in a way that ensures appropriate security, including protection against unauthorized or unlawful processing. Also, controllers must ensure that data cannot be modified by unauthorized persons.
5. **Storage limitation**. Personal data should be retained only while necessary. That is, personal data should be deleted once the legitimate purpose for which it was collected has been fulfilled. This is not simple, and needs to be determined in line with applicable laws that may sometimes require personal data to be retained for a longer period than the originally envisaged processing purpose.
6. **Fair and transparent.** GDPR asks that all personal data processing should be fair; that is, AGL does not perform processing that is not legitimate. Also, AGL should be transparent regarding the processing of personal data, and inform the data subject in an open and transparent manner. This means that personal data should be processed if, and only if, there is a legitimate purpose for the processing of that personal data. EU GDPR requires AGL to practice transparency so that data subjects will be sufficiently informed regarding the processing of their personal data

7. What the GDPR requires

While the Data Protection Directive only applied to data controllers, the GDPR now applies to data processors as well. Data controllers must now conduct Data Privacy Impact Assessments (DPIAs) and add more thorough methods of obtaining consent for collecting data.

Data processors will have to start keeping written records, increasing security measures to protect data and notify data controllers of any breaches that occur with the data.

The GDPR requires that clients of AGL are provided with thorough information about how their personal data is processed.

AGL will need to communicate information about how its processes personal data in a way that's:

- Concise
- Transparent
- Intelligible
- Easily accessible
- In clear and plain language
- Free of charge

This can be accomplished with a good Privacy Policy and privacy notices.

Access AGL's Privacy and Cookies Policy at https://abansglobal.co.uk/web/files/privacy-and-cookies-policy.pdf

8. GDPR Roles and Employees

AGL will have a designated Data Protection Officer (DPO) who will be responsible to implement the new data protection Regulation. The DPO and his team will be responsible for promoting awareness of the GDPR across the organization and assessing the robustness of our UK GDPR, identifying any gap areas and mitigating them in addition to implementing the new policies, procedures and measures.

9. Data Protection Principles

AGL will at all times follow the Eight Data Protection Principles, as originally established under the UK Data Protection Act 1998 (DPA 1998). These principles provide the foundation for handling personal data responsibly and ethically.

The eight Principles require that personal information:

1. shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;

2. shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
4. shall be accurate and, where necessary, kept up to date;
5. shall not be kept for longer than is necessary for the specified purpose(s);
6. shall be processed in accordance with the rights of data subjects under the Act;
7. should be subject to appropriate technical and organizational measures to prevent the unauthorized or unlawful processing of personal data, or the accidental loss, destruction, or damage to personal data;
8. shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

10. Data Breaches and their consequences

AGL is committed to maintaining the security and confidentiality of all personal data in its possession. In the event of a personal data breach—defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data—AGL will take immediate steps to mitigate any potential harm and comply with its obligations under the General Data Protection Regulation (GDPR) and UK GDPR.

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, AGL will:

- Notify the Information Commissioner's Office (ICO) (or the relevant supervisory authority) as soon as AGL becomes aware of the breach.
- Where the breach is likely to result in a high risk to the rights and freedoms of individuals, AGL will also communicate the breach to affected data subjects without undue delay.

All breaches, regardless of materiality, will be logged in a Data Breach Register, as required by law.

- Failure to protect personal data can result in:
- Reputational damage
- Legal liability, including regulatory fines (up to £17.5 million or 4% of annual global turnover under UK GDPR)
- Potential claims from affected individuals
- Regulatory enforcement action, including audits or formal investigations

AGL takes its data protection responsibilities seriously and regularly reviews its security controls, staff training, and incident response procedures to prevent and respond effectively to data breaches.