May 2018

Graydon's view on privacy

GRAYDON
open in business

Table of Contents

I. Introduction

The European General Data Protection Regulation (GDPR) lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. This regulation protects fundamental rights and freedoms of natural persons and in particular the right to the protection of personal data.

At Graydon, data is in the heart of our organisation. We live and breathe data and therefore we take GDPR very seriously. As it is our strategy to be a trusted partner in business, Graydon will be GDPR compliant by 25th May 2018.

Accountability is a very important principle within GDPR. Personal data may only be processed in a responsible manner. Because of Graydon's position as a party that holds a large amount of personal data and processes these as the core of its activities, it is essential to demonstrate this responsibility. Only then can Graydon be recognised as a reliable party both by the natural persons whose data are processed and by its business relations. This means companies need to demonstrate their compliance. This document gives an overview of our approach to GDPR.

II. What personal data is within Graydon

IExecuting our main activities are impossible without the processing of personal data. Since Graydon processes information about companies, their shareholders, directors and other company representatives, and on sole proprietors, we process significant volumes of personal related data. In addition, Graydon processes scores and ratings such as a credit score, produced from other information we have such as court judgments, financial accounts, and payment history information.

Depending on the data and processing activities, Graydon can be a controller (mostly) or a processor. For our own information database, we are a controller. This is because we exercise a high degree of control over our databases.

When we manage a customer database on behalf of a client, we act as a processor. We provide a service to the client but are not using this data for other purposes. The customer determines the purposes and makes use of Graydon services to achieve those purposes. When Graydon qualifies as a processor, it ensures that a data processor's agreement has been concluded with the customer as the data controller. This agreement specifies, among other things, which data Graydon processes for the customer and for which purposes.

III. How does Graydon make sure it becomes GDPR compliant in processing data?

1. Lawfulness, fairness & transparency

Legitimate ground for processing Personal Data

With regards to commercial data/Graydon's products & services:

- The legitimate ground for the processing of personal data as part of Graydon's products is legitimate interest (Art. 6 (f) GDPR).

With regards to clients and prospects

- The processing ground for personal information of clients and prospects is the consent (Art. 6 (a) GDPR) or performance of a contract (Art. 6 (b) GDPR).

Further explanation

As examples of Graydon's legitimate interest you can consider the interests we uphold to ensure financial sound and safe decision-making, the promotion of responsible lending, the prevention of fraud in order to help our customers and partners comply with regulatory obligations and prevent identity fraud / theft.

In the case of Graydon's customers and/or prospects, you can consider, for example, our responsibility to perform our obligation under a contract and to provide information on our products and services, insights in the latest market and business developments which are relevant for our prospects, business partners and customers.

In every situation, we have carefully considered the possible negative impact for data subjects involved and we have come to the conclusion that the way in which we process and the purpose for which we process this personal information is justified. In this assessment, we have made sure that we protect the data subjects and enforce proper security measures.

Transparency

Graydon is transparent about the data it processes and for which purposes this takes place. In order to provide adequate information, a clear Privacy Statement is available via the website. In addition, data subjects are actively informed about the processing of their personal data where possible. This vision paper itself also contributes to transparency by showing what measures Graydon is taking to be able to comply with the GDPR.

Data subjects also have rights that they can exercise in order to gain more insight in Graydon's data processing operations, such as the right of access. Graydon has set up procedures to facilitate these rights. This has been further elaborated below under 'Data subjects' rights'.

For transparency see 'right to information below' below.

2. Purpose Limitations

Our purposes are documented in our external Privacy Statement which can be found on our website and are referenced in our information notices (see 'right to information' and 'information duties' below), T&C's and other relevant documents. We will not further process personal

data for other purposes. All processing operations are subject to prior identification of their exact purposes, the reasons why they are necessary to achieve those purposes. And to an examination as to whether the purposes and the processing operations fulfil the requirements of lawfulness and proportionality.

3. Privacy by Design and Default

Graydon has implemented Privacy by Design & Privacy by Default within its business development and product development processes and departments. Graydon ensures that product development processes include Privacy by Design and Default requirements and assessments from conception until release, seeking to ensure the only data used in a product or service is the data required for that product or service and that the risks for the data subjects are mitigated. Privacy by Design & Default in the relevant departments which we have identified in this respect.

4. Accuracy

We live and breathe data. The best data quality is a key objective for our products and services. Our Operations department is continuously working on data quality and how to improve it. In order to maintain data quality, Graydon takes reasonable steps to ensure the accuracy of any personal data obtained by implementing policy and procedures in order to:

- Guarantee that the source of any personal data is clear;
- Carefully consider any challenges to the accuracy of information; and
- Consider whether it is necessary to (continuously) update the information.

5. Storage Limitation

The rationale with regards to retention is not changed by GDPR. All personal data that we process will fall under the retention policy that we will be implementing and referenced in our external Privacy Statement (to the extent it is relevant to data subjects) published online. Our retention policy has been drafted, having taken into consideration GDPR, other legal requirements, applicable Code of Conducts and other relevant standards and market practices.

6. Integrity & Confidentiality

We take security of personal data very seriously. We are committed to ensuring appropriate security is in place to prevent the personal data we hold being accidentally or deliberately compromised. Our IT Security Officer is dedicated and responsible for ensuring information security and we are currently working towards an ISO 27000 certification. In particular, we will:

- Design and organise our security to fit the nature of the personal data we hold and the harm that may result from a security breach;
- Make sure we have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and;
- Be ready to respond to any breach of security swiftly and effectively.

7. Accountability

The new accountability principle is one of the key changes that the GDPR introduces. In relation to this new principle, we will arrange for:

- Internal data protection policies (such as privacy policy, retention policy, data breach policy, HR privacy policy, information security policy, etc.);
- Employee communication and training programmes;
- Privacy audits;
- Adata asset register;
- Relevant Data Processing Agreements (DPA's) with our third parties;
- Data Protection Impact Assessments (DPIA's); and
- The appointment of a DPO.

IV. How can a data subject exercise their rights?

The GDPR provides data subjects with a broader set of new rights, giving them more control over what happens to their personal data. In short, we will:

(1) Provide data subjects with a clear explanation of their rights; how to exercise those rights and what they can expect to happen when they do.

(2) Have in place procedures for facilitating the exercise of the rights of data subjects by implementing policies and procedures within Graydon prescribing how to deal with requests from data subjects. There will be no unnecessary administrative hurdles and it will be operated by a local team of fully trained individuals who know what to do and have the authority to make things right if things have gone wrong.

(3) Publish online our Privacy Statement, the details about our appointed DPO, and make a Q&A available.

More information on the data subject rights will be provided in the next section.

V. Data subject rights

The right to information

A key principle in the GDPR is that data processing takes place in a transparent manner.

The duty to inform is focused on the data processing activities of Graydon. For instance: what we do, for what purposes, and based on what legitimate ground. In addition, it has to be clear for the data subject, which other organisations may receive personal data from Graydon, either as a processor or as a recipient.Graydon is a controller as the provider of several information products. Therefore, Graydon has to notify data subjects about their data being processed.

The information duties apply to all of Graydon's products. Even though for certain financial checks the information duty can be suspended, this only applies to Graydon's clients who use Graydon's Credit Information product(s) for these checks. This does, however, not influence Graydon's other duties.

Graydon will inform data subjects online in the form of a Privacy Statement by means of a letter to companies, by means of a Q&A on the website and by means of this document.

The right to access

Under the GDPR data subjects have the right of access. As the GDPR is daily in the news, it may be expected that the volume of requests will increase. The timescale for providing a response is one month. The right to access can be exercised by all categories of data subjects (i.e.. clients/prospects, persons in the commercial databases and employees) from whom personal data is processed by Graydon.

We are reviewing and revising our procedures for dealing with these kinds of subject access requests to ensure timely and correct processing of them within the new timescales.

Rectification

Under the GDPR the data controller must ensure that personal data are correct and accurate. Data subjects retain the right to obtain to data they consider to be incorrect or incomplete. Rectification is not a new right under the GDPR and Graydon already has a process in which a data subject can request a rectification. The right of rectification applies to all data subjects of which data is processed by Graydon.

Objection

The right to objection entails that any processing based on legitimate interests of the controller must generally be stopped unless there are compelling legitimate grounds which override the interests of the data subject raising the objection. Therefore, it is important to state for each process what the precise legitimate interests are for Graydon or a third-party. We have done so in our Privacy Statement. If the right of objection is invoked by a data subject Graydon will carefully weigh the interests of the involved party. In particular the rights and freedoms of the data subject against the interests of Graydon or a third party on a case by case basis. If Graydon is of the opinion that its interests take precedence over the interests of the party concerned, the latter will be informed thereof, including a careful substantiation of the outcome.

There is also a separate right for data subjects to object to the processing of personal data for direct marketing purposes. This is an absolute right and so, where we are using personal data for direct marketing, we will promptly comply with any objection received. This is only relevant for Graydon's clients/prospects.

Erasure / Right to be forgotten

The right to erasure (also known in the GDPR as the "right to be forgotten") is closely tied to the right to objection described above. It provides the data subjects with a right to have their data permanently erased, but only if the specified conditions are satisfied, and subject to certain exceptions.

For example, for credit referencing activity, it may be expected that most data subjects will not have sufficiently strong grounds to be able to have data erased on the basis of an objection to processing carried out by Graydon. This is because there will typically be compelling overriding grounds (as previously stated), primarily based on the importance of enabling lenders to make fair lending decisions, which justify that Graydon retains the data.

Restriction

The right of restriction is a right for data subjects means that processing must cease and the current status must be maintained (freezing of data).Data subjects have the right to have their personal data flagged as restricted (or under dispute) for example where they dispute the accuracy of information Graydon holds. The period for which the data must be flagged is the period of time needed to verify the accuracy.

However, even while the data is restricted, the GDPR permits it to be used for the protection of the rights of other individuals or organisations. The interests of other individuals or organisations must clearly outweigh the interest of the data subject concerned. In the majority of cases, we will therefore be justified in continuing to share data (marked as disputed) for credit referencing and other purposes, for instance to protect the legitimate rights of lenders to know about a person's bad credit history.

Data portability

The new right to data portability will rarely apply to Graydon. The right to data portability can be invoked when processing is based on consent or on a contract and the processing is carried out by automatic means (this may therefore only be relevant for clients/prospects and/or employees). Most of the processing within Graydon is done on the basis of legitimate interests (which does not trigger the right to data portability) and most of the data Graydon handles is obtained from third party organisations rather than from data subjects themselves. Where Graydon processes data on behalf of a client who may be under a data portability obligation, Graydon will assist the client to structure the data in a format required to comply with that obligation.

Automated decision-making

The data subject has a right under Article 22 of the GDPR not to be subject to a decision based solely on automated processing which significantly affects them. There are exceptions, such as where a data subject has given explicit consent. We are of the opinion that we do not make decisions which are subject to Article 22 of the GDPR. We supply information to our clients, and our clients use that information to make decisions (which may include automated decisions). We, therefore expect that our clients will want details about how the data we supply - such as credit scores - has been gathered or generated, and we are preparing materials to support such requests.

VI. How will we ensure compliance by others?

We have been reviewing existing supplier, customer and business partner contracts and, where necessary, these contracts will be amended to ensure compliance with the GDPR. Graydon aims to ensure that any new supplier, customer and business partner contracts will adhere to GDPR. To this end we have implemented related policies and processes that are integrated in our general purchase process.

VII. How will we ensure ongoing GDPR compliance from 25th May 2018?

Whilst it is important to achieve compliance with GDPR by 25th May 2018, the GDPR project we are running is just a starting point for continuous compliance with GDPR beyond that date. Maintaining compliance and further promoting careful use of data are crucial to Graydon's position and activities. Monitoring and audits will therefore continue to take place after 25 May. Procedures are regularly evaluated, and the DPO will monitor compliance with the GDPR internally. Finally, awareness is constantly being worked on in order to keep the knowledge of our employees up to date.

VIII. How will our products change as a result of GDPR?

We are reviewing our products as part of our GDPR project.

The products and services that clients purchase and receive from Graydon are being reviewed from a GDPR compliance perspective in order to identify what, if any, changes need to be implemented prior to 25th May 2018. As all of our products rely on "legitimate interest" as the lawful basis for processing personal data, this will still apply under the GDPR, we are confident that the vast majority of our products will continue to be available in the current form.

- There will be communications about the impact to particular products and timelines for client testing (where required) as soon as our plans are clarified. Further detail and guidance can then be obtained by working with the client facing teams.
- At the same time, we aim to ensure that our customer contracts reflect the new GDPR where required. We will also take this opportunity to simplify and standardise our contracts and terms and conditions.

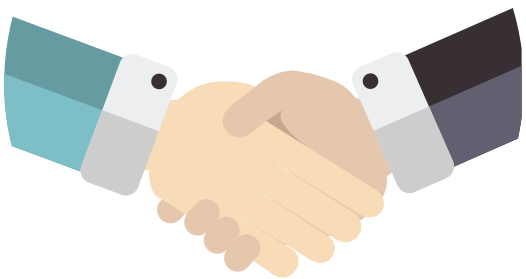
IX. How will our contracts change a result of GDPR?

Our standard client contracts and terms and conditions will be changing to take into account the new language and the new requirements of the GDPR.

Graydon will usually be acting as a controller rather than a processor.
Changes to our standard contracts will include:

- Being clearer about each party's status as a controller or a processor; and
- Updating the language to reflect the wording of the GDPR

These changes will be completed before 25th May 2018.



Graydon UK
2nd Floor – Hygeia Building , 66 College Road | Harrow, Middlesex HA1 1BE
T. +44 (0)20 8515 1400 | mail@graydon.co.uk