The UK General Data Protection Regulation (The UK GDPR) Policy

Introduction

The UK GDPR is retained in domestic law now the transition period has ended, but the UK has the independence to keep the framework under review. The 'UK THE UK GDPR' sits alongside an amended version of the DPA 2018.

The key principles, rights and obligations remain the same.

Our lead data supervisory authority is the Information Commissioner's Office (ICO).

As we decide how to process the data we collect on individuals, we are defined as a "data controller" by the ICO. This policy relates to Relendex Ltd.

Overview

The UK GDPR protects your personal data against the risks and losses caused by Cybers attacks which are an ever-growing problem. Failure to provide adequate data protection is a major reputational risk to the firm, and can result in fines and other potential serious consequences.

Awareness

Decision makers and key people in Relendex Ltd are trained to be aware of The UK GDPR provisions. As, Relendex currently employs fewer than 250 employees a Data Protection Officer is not required. The person responsible for data protection in the business is currentlyMax Lehrain.

Personal Data

Under The UK GDPR, “personal data” has a wide definition and includes identifiers such as an ID number, location data, online identifiers such as provided by devices, applications, tools and protocols such as IP addresses, cookie identifiers or other identifiers such as RFID tags.
Relendex Ltd must document what personal data is held, where it came from and who, if anyone, it is shared with. Currently, when personal data is collected, certain information needs to be given such as the firm’s identity and how the information is intended to be used.Under the UK GDPR additional information is required such as the legal basis for collecting the information, the data retention period and the fact that individuals have a right to complain tothe Information Commissioner’s Office if they think there is a problem with the way RelendexLtd is handling the information.

Six general principles regarding personal data

Relendex Ltd will follow the following six general principles:

1. Lawfulness, fairness, and transparency
2. Purpose limitation. Data must only be collected for a specified, legitimate purpose
3. Data minimisation. Data must be adequate, relevant, and limited to what is necessary
4. Accuracy. Data must be accurate and kept up to date
5. Storage limitation. Data must be kept in a form which permits identification of data subjects for no longer than is necessary
6. Integrity and confidentiality. Data must be processed in a manner that ensures appropriate security of the personal data including protection against unauthorised orunlawful processing and against accidental loss, destruction or damage by using appropriate technical or organisational methods.

Accountability

Relendex Ltd must demonstrate compliance with the six principles and appropriate governance measures must be in place.

Individual’s rights

Individuals have the right, under The UK GDPR, to subject access, correction of inaccuracies, information erasure, prevention of direct marketing, prevention of automated decision-making and profiling and data portability.

Our procedures in relation to these rights are below:

The right to be informed

Data subjects have the right to fair processing information and transparency over how we use their personal data. This information is brought to the attention of data subjects throughour privacy notices and privacy information contained in contracts.

The right of access

Under THE UK GDPR individuals have the right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data;
- Other privacy information (typically contained in a privacy notice).

The UK GDPR clarifies that the reason for allowing individuals to access the personal data wehold on them is so that they are aware of and can verify the lawfulness of the processing.

Individuals wishing to exercise their right of access may make a "subject access request" to Relendex Ltd using the contact details provided on our website. Following receipt of a subject access request the following procedure should be followed:

1. The individual should be contacted by the firm without delay, acknowledging receipt of their request. The firm should verify the identity of the individual at this point using 'reasonable means', which may involve answering security questions or using a secure token sent to their email or residential address.
2. If Relendex Ltd processes a large quantity of information on the individual, the firmcan ask the individual to specify the information the request relates to.
3. Relendex Ltd must provide the information:
   A. Within 30 days of the original request being received (which can be extended bya further two months if the requests are complex or numerous, in which case thefirm must contact the individual within one month of receiving the request and explain why the extension is necessary);
   B. Free of charge (unless the request is "manifestly unfounded or excessive");
   C. In a commonly used electronic format where possible, which may include remoteaccess to a secure self-service system;
   D. If a request is manifestly unfounded or excessive, which may include repeated requests for the same information, Relendex Ltd can either:
   E. Charge the individual a reasonable fee, which should be based on the administrative costs of providing the information; or

F. Refuse to comply with the request – in this case Relendex Ltd should contact the individual within 30 days and explain the reasons for refusal. This response should also inform them of their right to complain to a supervisory authority and the possibility of judicial remedies.

The right to rectification

The UK GDPR gives individuals the right to have their personal data rectified if it is inaccurate or incomplete.

Should Relendex Ltd receive a request for rectification the below procedure should be followed:

1. The individual should be contacted by the firm without delay, acknowledging receipt of their request. The firm should verify the identity of the individual at this point using 'reasonable means', which may involve answering security questions or using a secure token sent to their email or residential address.
2. Relendex Ltd should perform the necessary rectification within 30 days, which can be extended by a further two months in the case of a particularly complex request.
3. If the personal data in question has been disclosed to others, each recipient must be contacted and informed of the rectification, unless this proves impossible or involves disproportionate effort. If asked to, Relendex Ltd must also inform the individuals about these recipients.
4. If Relendex Ltd decides not to take action in response to a request for rectification, itmust explain why to the individual. The firm must also inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to erasure/right to be forgotten

In circumstances where there is no compelling reason for the continued processing of personal data, individuals may request the deletion of their data.

This right only applies in the following specific circumstances:

1. Where the personal data is no longer necessary in relation to the purpose for which itwas originally collected/processed;
2. Where the information was processed with the individual's explicit consent and the individual withdraws that consent;
3. Where the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
4. The personal data was unlawfully processed (i.e. otherwise in breach of the THE UK GDPR);
5. The personal data has to be erased in order to comply with a legal obligation;

6. The personal data is processed in relation to the offer of information society servicesto a child.

Relendex Ltd can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

1. To exercise the right of freedom of expression and information;
2. To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
3. For public health purposes in the public interest;
4. Archiving purposes in the public interest, scientific or historical research, or statistical purposes; or
5. The exercise or defence of legal claims.

Should an individual make a valid request for erasure, the data in question should be securely deleted immediately. If the personal data in question has been disclosed to others,Relendex Ltd should contact each recipient and inform them of the erasure of the personal data – unless this proves impossible or involves disproportionate effort. If asked to, Relendex Ltd must also inform the individuals about these recipients.

The right to restrict processing

Individuals have a right to block or suppress processing of personal data in some circumstances. Where Relendex Ltd has complied with a request for restriction, it may storethe personal data, but not process it further. The firm may retain just enough information about the information of the individual to ensure that the restriction is respected in future.

The right to restrict processing applies in the following circumstances:

1. Where an individual contests the accuracy of the personal data the firm holds, Relendex Ltd must restrict the processing until it has verified the accuracy of the dataor corrected it.
2. Where an individual objects to further processing, where the processing was necessary for the performance of a public interest task or in accordance with RelendexLtd legitimate interests, and the firm is considering whether its legitimateinterests override those of the individual.
3. Where processing is unlawful, but the individual concerned opposes erasure and requests restriction instead;
4. If the firm no longer needs the data but the individual requires the data to be held to establish, exercise or defend a legal claim.

If the personal data in question has been disclosed to others, Relendex Ltd must contact each recipient and inform them of the restriction on the processing of the personal data – unless this proves impossible or involves disproportionate effort. If asked to, Relendex Ltdmust also inform the individuals about these recipients.

Relendex Ltd must also inform individuals when it decides to lift a restriction on processing.

The right to data portability

This is a new right under The UK GDPR and refers to an individual's right to obtain and use their personal data for their own purposes across different services. This allows them to move,copy or transfer personal data easily from one IT environment to another in a safe and secure way.

This right only applies to personal data individuals have provided to Relendex Ltd (ratherthan data obtained from third parties), where the processing is based on the individual's consent or for the performance of a contract, and where the processing is carried out by automated means.

If an individual makes a request for data portability the following procedure should be followed:

1. The individual should be contacted by the firm without delay, acknowledging receipt of their request. The firm should verify the identity of the individual at this point using 'reasonable means', which may involve answering security questions or using a secure token sent to their email or residential address.
2. The data should be provided to them within 30 days, free of charge, in a "structured, commonly used and machine readable" format, such as CSV. This can be extendedby up to two additional months where the request is complex, or the firm receives several requests. The firm must inform the individual within one month of the receiptof the request and explain why the extension is necessary.
3. If the firm decides not to take action in response to a request, it must explain why to the individual within 30 days of receipt, informing them of their right to complain to the supervisory authority and the possibility of judicial remedy.

The right to object

There are some circumstances where individuals can object to further processing based ongrounds relating to their situation.

They can object to the following types of processing:

1. Processing based on legitimate interests or performance of a legal task (including profiling)
2. Direct marketing (including profiling)
3. Processing for purposes of scientific/historical research and statistics.

If the objection to the processing relates to the performance of a legal task or exercise of Relendex Ltd legitimate interest, the firm may only refuse such a request if it can demonstrate compelling legitimate grounds for the processing which override the interests,rights, and freedoms of the individual (note that this will be a narrow exception for private companies) or the processing is for the establishment, exercise, or defence of legal claims.

If an individual objects to personal data processed for direct marketing purposes, the Relendex Ltd must comply with this objection. There are no exceptions or grounds to refuse.

If the processing is carried out online, the individual must have the right to object online viasimilar means. In the case of direct marketing emails, this could be an “unsubscribe” link orsimilar.

Legal basis for processing

There must be a legal basis for gathering personal data and this reason must be disclosed inthe privacy notice. Where this legal basis is “explicit consent”, the consent of the data subject must be confirmed in the form of clear affirmative action. Additionally, the reason why the data is collected must be stated.

Individuals have the right to withdraw consent at any time and it must be as easy to withdrawas to give consent.

If Relendex Ltd has already gained consent, the firm is required to gain fresh consent underthe higher requirements of the The UK GDPR, if the previous consent was not up to The UK GDPR standards.

Data breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Under The UK GDPR, there is a

legal requirement to report data breaches. This must be completed without undue delay and, where feasible, within 72 hours.

If the breach is likely to result in high risk to the individuals, Relendex Ltd must also informdata subjects 'without undue delay' unless an exception applies.

There is a new requirement to retain an internal breach register.

Penalties

The maximum fine for The UK GDPR breaches is up to 2% of worldwide turnover or 10 million euros(whichever is the greater) for violations relating to internal record keeping, data protection officers and data protection by design and default.

Up to 4% of annual worldwide turnover or 20 million euros (whichever is the greater) for violations relating to breaches of the data protection principles, conditions for consent, data subject's rights and international data transfers.

Data subjects have the right to compensation from the controller or processor where theysuffer material or non-material damage (such as distress) due to a breach of the The UK GDPR.