ICAEW KNOW-HOW
BUSINESS LAW
GDPR AND THE DATA PROTECTION ACT 2018

THE RIGHT TO ERASURE

GUIDE

January 2020

The EU General Data Protection Regulation (GDPR) came into force on 25 May 2018. The Data Protection Act 2018 (DPA 2018) came into force on the same day and sits alongside the GDPR. This guide is part of a series that explain some of the new or more difficult concepts introduced by the GDPR and DPA 2018. It is intended to provide practical guidance to ICAEW members. It is not intended to constitute legal advice. If in doubt members are advised to consult with the Information Commissioner's Office (ICO) and/or seek legal advice

Introduction

The GDPR affords data subjects the right to request the erasure of their personal data and obliges data controllers to comply with their request in some circumstances but not all.

This guide summarises the general erasure obligations set out in GDPR, the exceptions available under GDPR and the DPA 2018 and provides practical interpretation of these in relation to various example service offerings that may be provided by ICAEW members.

Members should also consider their obligations as ICAEW members regarding the retention of documents and records, including client files. – see here for further guidance.

What is the right to erasure?

Data subjects (individuals) have a right to the erasure of their personal data under Article 17 of the GDPR –the so called 'right to be forgotten'. In common with other data subject rights, this right is not absolute as it only applies in certain circumstances.

The right to erasure must be communicated to individuals whenever their personal data is processed. In practical terms this is normally contained within an organisation's privacy notice either available to the individual on its website or communicated to them during the collection of personal data.

On receipt of an erasure request, the organisation should acknowledge the request from the individual promptly and then process the request, providing a response to the individual within one month of the request. Comparable obligations to the right of access (see here for further guidance) apply to the request such as assuring the identification of the requestor.

When does the right of erasure apply?

The right of erasure applies in the following circumstances:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;

- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- you must do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

The GDPR[1] permits the retention of personal information if it is necessary for the establishment, exercise or defence of legal claims under the organisations' legitimate interest. When relying on a legitimate interest you will have to consider how you meet your transparency obligations. [insert link to transparency guidance]

Do I have to inform anyone of the fact that the right to erasure has been requested and complied with?

Where the right of erasure applies and you have provided the personal data to other organisations, you must contact each recipient and inform them of the erasure request, unless this proves impossible or involves disproportionate effort. When asked by the individual, you must also inform them about these recipients.

What about backup systems – do I need to erase data stored in this way?

Where the right of erasure applies, you will need to consider where the data exists. An area of practical difficulty is erasing data from backup systems. Provided the personal data held in the backup system is only used for backup purposes it will be low risk to the individual. Where this data cannot be erased it will likely suffice to have procedures in place that in the event of a backup restoration, the data subject to the right of erasure is erased at the time of restoration.

What if someone objects?

You will need to consider any interplay between the rights of erasure, and objection. If an individual objects and you are relying on your or a third parties' legitimate interest, you will need to consider whether those interests outweigh the rights and freedoms of the individuals.

Can I refuse a request?

Yes, but where you refuse a request for erasure you should explain your reasons for refusal, your complaints process and ultimately the data subject's right to complain to the ICO or seek a judicial remedy.

See the Appendix for practical examples of what you should do in a variety of common situations

[1] Article 17(3)(e)

Where can I find out more?

- For detailed advice read:
  - EU General Data Protection Regulations (GDPR)
  - Data Protection Act 2018 (DPA 2018)
  - The ICO's guidance on Data Subject Rights
  - The European Data Protection Board's (formerly the Article 29 Data Protection Working Party) Guidelines
- For more general advice on all aspects of the DPA 2018 and GDPR, see the ICO's Guide to Data Protection
- For more support, visit ICAEW's GDPR hub and Data Protection webpages
- Members should also consider their obligations as ICAEW members regarding the retention of documents and records – see here

APPENDIX

Practical examples

In order to illustrate the above circumstances, it may be useful to consider the following examples.

I. A failed job applicant

A failed job applicant requests for their data to be erased. The organisation collects and retains complete records of all applicants, their application process and notes of the various stages of the process. If the applicant is successful, the data moves into their HR files and forms part of the employee file. Where the application fails, the organisation holds the full data for 6 months in order to defend any legal claims relating to discrimination and further holds the identification data of the individual for 2 years to assess if the applicant applies again within that time period as they have a policy of not accepting applications from failed applicants for 2 years.

If the applicant requests the erasure of their data, the following circumstances will apply:

If requested prior to 6 months of the conclusion of the application process, the organisation would likely rely on its need to keep the personal data under its legitimate interest of defending a potential legal claim. As the time limit for making a claim for discrimination is 6 months from the day when the discrimination is alleged to have taken place, the legitimate interest should be in balance.

If the request is prior to the two years then all personal data should be erased except for the identification data (possibly forename, surname, date of birth, application date, application role). The organisation would rely on its legitimate interest to hold such personal data to enforce its policy of not accepting applications from failed applicants for a two-year period. The legitimate interest will only cover certain elements of personal data and other information should not be retained unless necessary such as for example references, interview notes and background checks.

Where their personal data has been passed to another organisation for example to undertake background checks, then the latter must be informed of the request to have such data erased.

II. An ex-employee

An ex-employee requests their HR records are deleted after they leave the organisation

The organisation has a retention policy which retains all personal data of an employee for 7 years post termination in order to meet its legal obligations for record keeping. A number of other elements of the personnel file are held for longer such as “records relating to pre-employment health screening for employees exposed to hazardous waste during employment” where the retention period is 40 years[2]. An ex-employee exercises their right to erasure. Where the data is covered by the record retention policy based on a legal obligation the request can be refused. Where the organisation holds personal data and there is no reason to do so post-employment such as details of next of kin, the data should be erased within one month of the request.

III. A personal client

A personal client requests their data be erased.

One of the legal bases on which the personal data of the personal client is undertaken is when the processing is necessary for a contract the organisation has with the individual. There may also be a legitimate interest of the organisation to retain records in compliance with its professional

[2] Control of Asbestos at work regulations 2002, Control of Lead at work regulations 2002, Control of Substances Hazardous to Health Regulations 2002

obligations (eg as a member firm of ICAEW) or as a result of a legal obligation conferred through legislation.

In such cases it is unlikely that data would be erased until the later of the retention obligations are reached.

IV. Inclusion on a client database

A client who previously attended a corporate event asks not to be contacted again in relation to future events and their data erased.

The lawful basis for further processing of the client' s personal data is likely based on consent or the organisation's legitimate interest. If consent is the basis, the request should be treated as a withdrawal of consent and the data erased. If relying on your or a third party's legitimate interest, then Article 21(3) states that the personal data shall no longer be processed for such purposes. In both cases the right of erasure would apply.

Where you hold some information to identify that the individual has objected to your organisation processing their personal data for direct marketing, you are able to continue to hold a limited record to ensure you do not contact them again in the future.

© ICAEW 2020

All rights reserved.
If you want to reproduce or redistribute any of the material in this publication, you should first get ICAEW's permission in writing.
ICAEW will not be liable for any reliance you place on the information in this material.
You should seek independent advice.

ICAEW is a world leading professional membership organisation that promotes, develops and supports over 150,000 chartered accountants worldwide. We provide qualifications and professional development, share our knowledge, insight and technical expertise, and protect the quality and integrity of the accountancy and finance profession.

As leaders in accountancy, finance and business our members have the knowledge, skills and commitment to maintain the highest professional standards and integrity. Together we contribute to the success of individuals, organisations, communities and economies around the world.

Because of us, people can do business with confidence.

ICAEW is a founder member of Chartered Accountants Worldwide and the Global Accounting Alliance.
www.charteredaccountantsworldwide.com
www.globalaccountingalliance.com.

Chartered Accountants' Hall
Moorgate Place, London
icaew.com

T +44 (0)20 7920 8100
E generalenquiries@icaew.com

TECPLN15834