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

TRANSPARENCY

GUIDE

April 2019

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.

Introduction

The GDPR obliges data controllers to be transparent with data subjects about how they process their personal data. However, given the nature of some of the services provided by ICAEW members, this obligation to be transparent may appear to be unworkable, inappropriate or even not feasible in some circumstances.

This guide summarises the general transparency 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.

What is transparency?

Transparency is included in Article 5.1 of the GDPR as one of the principles relating to the processing of personal data, "*Personal data shall be processed lawfully, fairly and in a **transparent** manner in relation to the data subject".* This means that data subjects should be provided with sufficient information to enable them to understand, and if appropriate challenge, how their personal data is being processed. In addition, transparency covers how data controllers communicate with data subjects in relation to their rights under GDPR and how they facilitate the exercise by data subjects of such rights.

The accountability principle contained in Article 5.2 requires that controllers must be able to demonstrate that personal data is processed in a transparent manner. In addition, Article 24 requires controllers to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR.

What are the transparency requirements?

Transparency obligations are predominantly set out in Articles 12, 13 and 14 of GDPR. The responsibility to fulfil these obligations rests with the data controller. Therefore, where ICAEW members are solely providing a data processing service to a client, such as when providing IT processing services, it is the client that is responsible for establishing appropriate transparency with data subjects; in such situations, ICAEW members must make it clear in the engagement letter that the responsibility for transparency rests with the client as the data controller.

Article 12 of GDPR requires that information provided to and communications with data subjects:

- are in a concise, intelligible and easily accessible form;

- use clear and plain language;
- are provided in writing or by other means including, where appropriate, electronic: and
- are provided free of charge.

Articles 13 and 14 set out the information that must be provided to data subjects where personal data is collected from the data subject (Article 13) and where personal data has not been obtained from the data subject (Article 14). The requirements of each are broadly similar and are specific in the types of information to be provided to the data subject. These include information about the controller, the processing activity, the personal data being processed and the rights available to the data subject.

The most common means of providing the above information to data subjects is via a privacy notice (see below). This should be made available to data subjects when collecting the personal data or, when personal data is not collected from the data subject, at the latest when (i) first using the personal data for communicating with the data subject, (ii) first disclosing the personal data to another recipient, or (iii) within one month of obtaining the data.

Should a data controller intend to process personal data for a new purpose (ie, a purpose other than that for which the personal data was originally obtained), then information relevant to that other purpose should be provided to the data subject prior to processing.

Are there any exceptions?

Exceptions to the data subject's right to information exist under Articles 13 and 14 of GDPR. In addition, the restrictions on data subject rights set out in Article 23 may apply.

A summary of the exceptions most relevant to ICAEW members and their origin is included in Appendix 1. Examples of the more common situations where exceptions may be available are provided below.

What is a privacy notice?

Privacy notices are commonly used to provide the necessary information to data subjects concerning the processing of their personal data. In addition to the provision of a privacy notice to data subjects when personal data is collected, it is recommended that all ICAEW members publish a privacy notice on their websites explaining how they process personal data. The privacy notice should be comprehensively drafted and contain the information specified under Articles 13 and 14. ICAEW guidance on the content of privacy notices can be found here.

Where personal data is collected from the data subject, then the provision of the privacy notice to the data subject at the time of collecting the data should enable compliance with Article 13.

Where personal data is collected from corporate clients rather than directly from data subjects, the privacy notice should be provided to the data subject either when first communicating with the data subject, when first disclosing the personal data to another recipient or within one month. If this is not feasible and it is considered that the "disproportionate effort" exception (see Appendix 1) is applicable, it is recommended that efforts still be taken to establish "pathways" that can be followed by data subjects to allow them, if interested, to understand how their personal data may be being processed by members. This can most readily be achieved by the client including reference within their own privacy notice to the potential transfer of personal data held by them to the ICAEW member for the provision of services, such as audit, and it is recommended that such an obligation is included in the contract between the ICAEW member and the client. Interested data subjects will then know to refer to the member's publicly available privacy notice to understand how their personal data may be being processed and how to exercise their rights.

You must regularly review and, where necessary, update your privacy notice for any new uses of personal data. Unless a valid exception applies to new processing, you must bring any changes to the attention of data subjects before you start the processing.

What are practical examples of exceptions?

Details of exceptions that might be available are set out at Appendix 1. Situations where these might be applicable are described below. Each must be decided on a case by case basis.

Audits

During an audit personal data relating to shareholders, suppliers, customers, employees and others may be processed by the auditor when forming an opinion on the financial statements. For the most part, the personal data is not collected from the data subject, and Article 14 will apply. Processing of personal data within an audit is of a verification nature and is not designed to have any new impact on the data subject (though clearly may result in corrective action should inaccuracies in the client's original processing activities be revealed); this is similar to processing conducted for archiving, research and statistical purposes. Therefore, whilst it might be possible to provide data subjects with information, to do so would involve a level of effort disproportionate to the intended impact on the data subject, and, in the absence of exceptional circumstances, the "disproportionate effort" exception may be expected to apply. The auditor must however make the information required in Article 14 publicly available, preferably by use of a privacy notice (see above), and the client should include reference of the potential transfer of personal data to the auditor in their own privacy notice (it is recommended that the engagement letter obliges the client to do this).

Other attestation services

Where ICAEW members provide other independent attestation services, for example client money audits, gender pay gap reporting and reports under SSAE 18, it is likely that circumstances similar to those in an audit will apply; notably, there will be no intended impact on the data subjects whose personal data may be processed as part of the engagement and that contacting data subjects directly will involve a substantial effort. As such, in the absence of exceptional circumstances, the "disproportionate effort" exception may be expected to apply. The ICAEW member must however make the information required in Article 14 publicly available, preferably by use of a privacy notice (see above), and the client should include reference of the potential transfer of personal data to the ICAEW member in their own privacy notice (it is recommended that the engagement letter obliges the client to do this).

Corporate finance services

Where ICAEW members provide corporate finance related services to publicly listed companies, such as when providing long form, short form or working capital reports in relation to a new listing or rights issue or advice in relation to mergers and acquisitions, it is possible that they may process personal data relating to shareholders, suppliers, customers, employees or other data subjects of the issuer or, where relevant, the acquisition target. Such personal data will generally be collected from the issuer, acquirer or target, and Article 14 will apply. Such processing is subject to confidentiality obligations so as not to affect the price of any financial instrument, the orderly functioning of financial markets or efficient allocation of capital in the economy. The "corporate finance" exception available under DPA 2018, Schedule 2, Part 4, para 21 may be expected to apply.

Due diligence services

ICAEW members also frequently undertake pre-acquisition due diligence reviews on behalf of unquoted clients (or which otherwise do not meet the conditions of the "corporate finance" exception above) during which they may process personal data relating to shareholders, suppliers, customers, employees or other data subjects of the intended acquisition target. Such personal data

will generally be collected from the acquisition target organisation and Article 14 will apply. In nearly all circumstances, the content of working papers and reports relating to such services are confidential as they will be used in the preparation of management forecasts and planning for the proposed transaction; this will especially be the case if the transaction is not public knowledge. Informing data subjects about the processing activity would therefore be likely to prejudice the intended transaction, and the "Management forecast" exception available within DPA 2018, Schedule 2, Part 4, para 22 may be expected to apply.

Forensic and other investigations

Where ICAEW members are engaged to provide investigative services, for example in response to a regulatory or legal enquiry, they may process a variety of personal data belonging to various types of data subject, often in large quantities. For many investigatory services, the purpose and means of processing will be determined by the client (or their legal adviser) and the ICAEW member will be acting as data processor only and not responsible for transparency. However, there may also be circumstances where the member has a degree of independence in determining the purpose and means of processing and would be a controller in their own right and responsible for transparency. Depending on the nature of the investigations, various exceptions may be considered.

- Under DPA 2018, Schedule 2, Part 1, para 2(1), information does not need to be provided to the data subject where doing so is likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.
- Under DPA 2018, Schedule 2, Part 2, para 7, information does not need to be provided to data subjects where doing so is likely to prejudice functions designed to protect the public interest. More details on this exception are provided in the Appendix, which could apply where the investigation is designed to protect the public or charities against financial loss due to dishonesty, malpractice or improper conduct.
- Under DPA 2018, Schedule 2, Part 2, paras 8, 9, 10 and 11, information does not need to be provided to data subjects where doing so is likely to prejudice investigations performed on behalf of various statutory and regulatory bodies.
- Under DPA 2018, Schedule 2, Part 2, para 14(3), information does not need to be provided to data subjects if the provision of such information is likely to prejudice judicial proceedings.
- Under DPA 2018, Schedule 2, Part 4, para 23, information does not need to be provided to a data subject where the investigation is in relation to that subject and informing them may prejudice negotiations with the data subject.
- Under GDPR Article 14, para 5(b), information does not need to be provided to the data subjects where it is impossible (such as when the ICAEW member has access only to pseudonymised data) or would involve a disproportionate effort. In relation to the latter, a balancing exercise would be required to balance the extent of effort required with the impact on the data subject; this may conclude, especially when analysing large data sets to identify specific exceptions, that the provision of information to data subjects is only required if the investigation results in an impact on a data subject.

Consulting services

Certain consulting services may involve the processing of personal data, particularly those relating to organisational and human capital management. Where the purpose of such processing is in relation to management forecasting or planning and the provision of information is likely to prejudice the activity concerned, the "Management forecast" exception available within DPA 2018, Schedule 2, Part 4, para 22 may be expected to apply. This is likely to be the case, for example, where redundancy or reorganisation programmes are being considered.

Do exceptions cover other data subject rights or just transparency?

This depends on the source of the exception. Those in Article 14 are limited to the provision of information to data subjects when personal data is not collected from the data subject. The exceptions arising from the DPA, Schedule 2 also apply to Article 15 "*Right of access"* and, in certain circumstances, other rights such as Article 16 "*Right of rectification",* Article 17 "*Right to erasure",* Article 18 "*Right to restriction of processing"*, Article 19 "*Notification obligation regarding rectification or erasure of personal data or restriction of processing*", Article 20 "*Right to data portability"* and Article 21 "*Right to object"*, but not all are applicable to all those services. If in doubt, members should refer to the DPA to see which GDPR provisions are exempted or obtain their own independent legal advice.

What do I need to do if an exception applies?

Although the above exceptions are available for use, it is best practice to be as transparent as possible, proportionately to the rights and obligations members have to their clients. If an Article 14 exception applies, the controller must still take appropriate measures to protect the data subject's rights and freedoms and legitimate interests. This will include ensuring that appropriate technical and organisational measures are in place to protect the security of the data. In addition, information regarding the processing should be made publicly available; this can be done by making a comprehensive privacy notice available on websites.

In addition, in order to comply with the "accountability" requirement in GDPR, it is recommended that members make contemporaneous records of the reasons why they make certain decisions on the applicability of an exception(s).

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 Transparency and Privacy Notices
  - The European Data Protection Board's (formerly the Article 29 Data Protection Working Party) 'Guidelines on transparency under Regulation 2016/679'
- 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
- For advice on engagement letters and privacy notices, see ICAEW's Engagement Letters Helpsheet

APPENDIX 1

EXCEPTIONS TO TRANSPARENCY REQUIREMENTS IN THE GDPR

Articles 13 and 14 exceptions:

A general exception exists under Articles 13 and 14 whereby no information needs to be provided insofar as a data subjects already has the information. For example, if the necessary information is provided to the data subject when they subscribe for a service, the same information does not need to be provided each time personal data is obtained in connection with provision of that service.

Article 14 contains further exceptions that apply only where the data is not collected from the data subject. These are:

- where the provision of the information *proves impossible, involves a disproportionate effort or would seriously impair the objectives of processing*;
- where obtaining or disclosing personal data is expressly laid down by a *rule of domestic law*; and
- where the personal data must remain confidential subject to an obligation of *professional secrecy*.

Proves impossible, disproportionate effort or serious impairment of objectives

In practice, there are likely to be few situations where the controller can demonstrate that it is *impossible* to provide the information to data subjects, though this exception could be valid in situations where, for example, the controller does not have and it is not possible to obtain contact details for data subjects (eg, when the controller is processing pseudonymised data, but is not able to identify individuals). Should the factors causing the impossibility cease to exist, then the information should be provided to the data subjects immediately.

The European Data Protection Board's guidelines on transparency indicated that its position regarding the *disproportionate effort* exception was that it should not be used routinely unless in relation to archiving, research or statistical purposes. However, the wording of Article 14(5) (b) does not limit the use of the disproportionate effort exception to processing for archiving, research or statistical purposes, it refers to such processing as examples of areas where the disproportionate effort exception may apply. If this exception is to be relied on, a balancing exercise should be undertaken by the controller to assess the effort required against the potential impact and effect on the data subject by not having the information taking into account the number of data subjects, the age of the data and any appropriate safeguards adopted.

The *serious impairment of objectives* exception may apply in certain legal or obligatory reporting situations, such as when making suspicious activity reports under anti-money laundering regulations.

Rule of domestic law

This exception applies where obtaining or disclosing personal data is expressly laid down by domestic law. It is thought to have limited application in relation to services provided by ICAEW members, though it would cover matters such as the statutory requirement to provide details on employees to the Revenue (for tax purposes) or to the Home Office (to comply with immigration law).

Professional secrecy

This exception only applies where the obligation of professional secrecy is regulated by domestic law, including a statutory obligation of secrecy. As such, it is thought to have limited application for ICAEW members.

Regardless of whether exceptions are available, the processing of personal data must be fair, have a proper legal basis and appropriate measures must be taken to protect the data subject's rights and freedoms and legitimate interests. In respect of the *impossibility* or *disproportionate effort* exceptions, this includes a requirement to make the necessary information public, for example by publication on a website, advertising in newspapers or posters on premises.

When relying on an exception, to comply with the accountability principle the controller should undertake and document an assessment of why the exception is appropriate.

Article 23 restrictions on data subject rights

Article 23 permits member states to restrict by legislation the scope of data subject rights; this includes the transparency obligations on controllers. The UK has set out various exceptions within Schedule 2 of the Data Protection Act 2018. These are extensive. The most relevant to ICAEW members are set out below.

Crime and taxation (DPA 2018, Schedule 2, Part 1, para 2)

An exception exists where providing information to a data subject is likely to prejudice the prevention or detection of crime, the apprehension of prosecution of offenders or the assessment or collection of tax.

Functions designed to protect the public (DPA 2018, Schedule 2, Part 2, para 7)

Various functions are detailed that, where conferred on a person by an enactment or of a public nature and exercised in the public interest, are exempt (among other matters) from the obligation to provide information to data subjects to the extent that doing so would be likely to prejudice the proper discharge of the function. These functions include those designed:

- *to protect members of the public against (a) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate, or (b) financial loss due to the conduct of discharged or undischarged bankrupts.*
- *to protect members of the public against (a) dishonesty, malpractice or other seriously improper conduct, or (b) unfitness or incompetence.*
- *(a) to protect charities or community interest companies against misconduct or mismanagement (whether by trustees, directors or other persons) in their administration, (b) to protect the property of charities of community interest companies from loss or misapplication, or (c) to recover the property of charities or community interest companies.*
- *(a) to secure the health, safety and welfare of persons at work, or (b) to protect persons other than those at work against risk to health or safety arising out of or in connection with the action of persons at work.*

Audit functions (DPA 2018, Schedule 2, Part 2, para 8)

An exception exists for personal data processing for the purpose of discharging a function of the Comptroller and Auditor General, the Auditor General for Scotland, the Auditor General for Wales, the Comptroller and Auditor General for Northern Ireland and provision of information is likely to prejudice the proper discharge of the function.

Other regulatory functions (DPA 2018, Schedule 2, Part 2, paras 9, 10 and 11)

An exception exists for personal data processing for the purpose of discharging relevant functions of the Bank of England, regulatory functions relating to legal services, the health services and children's services and regulatory functions of certain other persons to the extent that the provision of information is likely to prejudice the proper discharge of the function. Other regulatory functions include the ICO, the Pensions Ombudsman and other pension regulators, the Financial Conduct

Authority and Financial Ombudsman, the Public Services Ombudsman and the Charity Commission.

Legal professional privilege (DPA 2018, Schedule 2, Part 4, para 19)

An exception exists for personal data that consists of information in respect of which (a) a claim to legal privilege (or, in Scotland, confidentiality of communications) could be maintained in legal proceedings, or (b) a duty of confidentiality is owed by a professional legal adviser to a client of the adviser.

Corporate finance (DPA 2018, Schedule 2, Part 4, para 21)

An exception exists for personal data processed in relation to corporate finance services. This exception is however restricted to where the provision of information to data subjects would need to be likely to affect the price of a financial instrument, the orderly functioning of financial markets or efficient allocation of capital in the economy.

Management forecasts (DPA 2018, Schedule 2, Part 4, para 22)

An exception exists for personal data processed for the purposes of management forecasting or planning in relation to a business or other activity to the extent that the provision of information to data subjects would prejudice the conduct of the business or activity concerned.

Negotiations (DPA 2018, Schedule 2, Part 4, para 23)

An exception exists for personal data that consists of records of the intentions of the controller in relation to any negotiations with the data subject to the extent that the provision of information to the data subject would prejudice those negotiations.

Confidential references (DPA 2018, Schedule 2, Part 4, para 23)

An exception exists for personal data consisting of a reference given in confidence for the appointment of the data subject to any office or the provision by the data subject of any service.

As with the Article 14 exceptions, when applying one of the Article 23 restrictions to data subject rights controllers should ensure the processing of personal data remains fair, has a proper legal basis and appropriate measures are be taken to protect the data subject's rights and freedoms and legitimate interests. In addition, to comply with Article 5.2, it is recommended that an assessment justifying why the restriction is appropriate is documented.

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