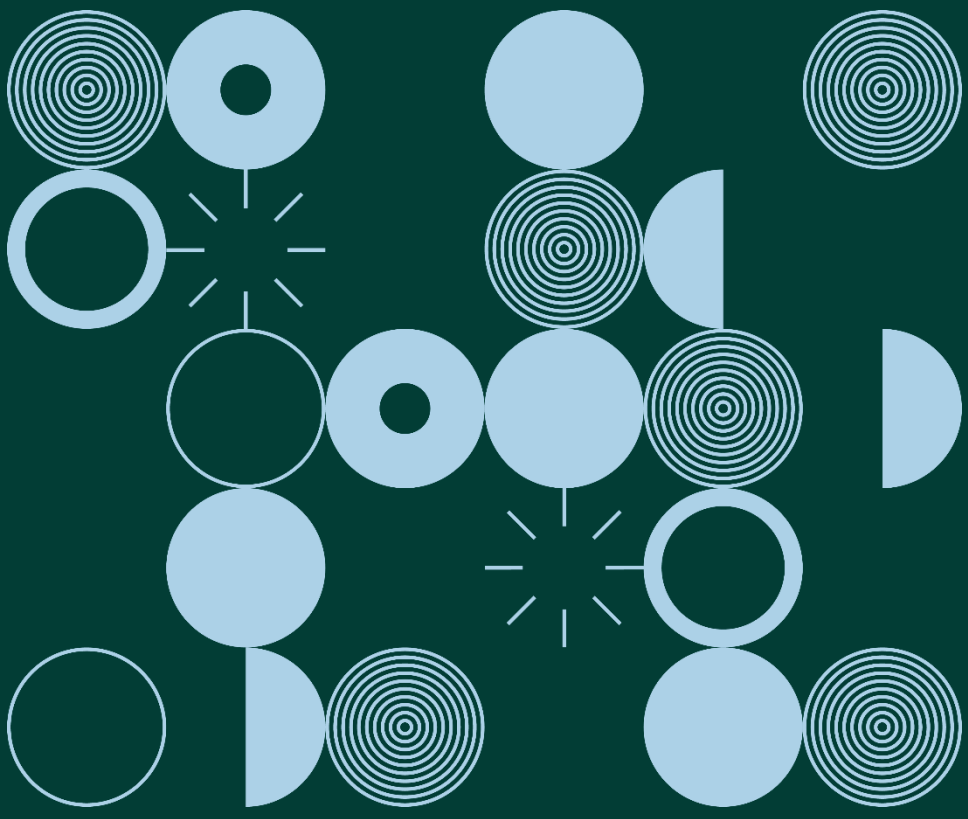
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Guidance Note:

Guidance on Transfers of Personal Data from Ireland to the UK in the Event of a 'No-Deal' Brexit

October 2019



Contents

Steps to determine whether you are a controller that transfers personal data to the UK (including Northern Ireland)

Brexit, particularly in the context of a 'No Deal' scenario, may have a significant impact on the data protection obligations of Irish entities which transfer personal data to the UK (including Northern Ireland).

The following is a non-exhaustive list of **ways you might be transferring data to a UK-based company**, which potentially affected controllers should consider:

- ☐ Are you **outsourcing** your HR, IT or Payroll function to a UK-based organisation?
- ☐ Are you using a UK-based **marketing** company to send marketing communications to your customer database?
- ☐ Is your **occupational health provider** based in the UK?
- ☐ Is your **pension scheme** based in the UK?
- ☐ Are you using **translation/transcribing services** of a UK based company where you might be sending personal data of employees, customers or suppliers?
- ☐ Are you using a UK-based company to **analyse data on visitors** to your website?
- ☐ Are you storing data in the UK on a **server or in the cloud**?

Measures required to legally transfer personal data from Ireland to the UK in the event of a 'No Deal' Brexit

With the advent of the GDPR in particular, countries in the EU have very high standards of data protection. EU-based data controllers are not permitted to transfer personal data outside the EU/EEA unless those **standards are maintained**.

Below are some considerations of how a 'No Deal' Brexit will change the status of the UK as a destination for transfers of personal data, and what steps might be required to ensure adequate protection of any personal data which is transferred.

The UK as a 'Third Country'

In a 'No Deal' Brexit scenario, the UK will no longer be a member of the EU; instead, it **will become a 'third country'**. This means that transfer of personal data from Ireland to the UK will be treated in the same way as transfers of personal data to countries like Australia, India, or Brazil.

What this means in practice is that, in order to comply with GDPR rules, an Irish company intending to transfer personal data to the UK will need to put in place **specific safeguards** to protect the data in the context of its transfer and subsequent processing.

This can be done in a number of different ways, depending on the circumstances in which the data is to be transferred.

Standard Contractual Clauses (SCCs)

One such measure for ensuring the protection of personal data transferred to the UK is the use of 'standard contractual clauses' or 'SCCs', and this is likely to be relevant to most Irish businesses that transfer personal data to the UK.

The SCCs consist of **standard or template sets of contractual terms** and conditions that the Irish-based controller and the UK-based recipient (often acting as a data processor) both sign up to.

The basic idea is that each of the parties to the contract gives **contractually binding commitments** to **protect personal data** in the context of its transfer from the EU/EEA to the Third Country. Importantly, the **data subject** is also

given certain **specific rights** under the SCCs even though he or she is not party to the relevant contract.

The SCCs can be adopted by putting in place a **stand-alone or new contract** between the Irish-based controller and the UK-based recipient. As well as setting out the SCCs, that contract may **also include other commercial clauses** *provided* those other clauses **do not affect the operation of the SCCs or reduce data subjects' rights**.

Likewise, any additional commercial clauses must not reduce the level of protection which the UK-based entity is required to provide for the transferred data. An example of the kind of commercial clause that is permitted is a provision under which the UK entity indemnifies the Irish controller against a breach by the UK entity of its obligations under the contract.

Alternatively, where the Irish-based controller and UK-based processor **already have a contract in place** between them, as required by Article 28(3) of the GDPR, they may **decide to incorporate the SCCs** into that existing contract. Again, this is provided that its terms do not affect the SCCs or reduce the data subject's rights, and provided its terms do not reduce the level of protection which the UK processor is required to provide for the transferred data. Depending on the particular form and terms of their existing contract, this outcome could be achieved by means of a written variation.

A **sample set of Standard Contractual Clauses** (Controller to Processor, 2010) can be found on the DPC website. These clauses (which were developed by the European Commission) can be used if you are an Irish data controller who is transferring personal data to a UK-based service provider, where your service provider is acting as a data processor. The European Commission has also produced SCCs for transfers from an EU controller to a non-EU or EEA controller – all three sets of SCCs can be found on the European Commission website.

Overview of the contents of standard contractual clauses

The follow represents a very brief over-view of the contents of the SCCs:

- On the **first page**, the parties to the SCCs contract are required to insert certain basic information, identifying the name and contact details of the "data exporter" (Irish based controller) and the "data importer" (UK based service provider).
- **Clause 1** then defines certain key terms. You will see that this clause refers to Directive 95/46/EC rather than the GDPR. This reflects the fact that this particular template was developed prior to the adoption of the

GDPR. The GDPR provides that the template remains valid, however, unless and until the EU Commission replaces it.

- Details of the transfer must be inputted into ***Appendix 1*** of the Contract (see further below). **Clause 2** is important because it incorporates the information set out at ***Appendix 1*** into the contract itself.
- **Clause 3** establishes certain rights for the data subject, even though he/she is not a party to the contract.
- **Clause 4** sets out the data exporter's obligations, i.e. the commitments to be given by the Irish-based controller. These should be carefully examined.
- **Clause 5** then sets out the data importer's obligations, i.e. the commitments being given by the UK-based service provider.
- **Clause 6** deals with issues of liability as between the data exporter and importer.
- In **Clause 7**, the data importer acknowledges that if, in a dispute situation, the data subject exercises its rights under Clause 3, it will be for the data subject to decide whether to mediate the dispute or to bring a legal action in the courts of the member state in which the data exporter is based (i.e. Ireland in this case).
- In **Clause 8**, the data exporter and data importer commit to co-operating with the relevant supervisory authority (in this case, Ireland's Data Protection Commission).
- At **Clause 9**, the parties should insert "Ireland" as the member state whose laws will apply to the contract.
- **Clause 10** notes that the parties may add additional clauses, but only if those clauses do not vary or modify the SCC clauses themselves.
- **Clause 11** deals with certain issues relating to the position of sub-processors engaged by the data importer.
- **Clause 12** sets out the parties' obligations when the processing services being provided by the data importer come to an end.

Following the signature block, the document then has two appendices.

Appendix 1

At Appendix 1 the parties to the contract must set out details of the transfer itself. This section of the document is of critical importance and is organised under 6 different headings:

- *Heading #1* – "**Data Exporter**"
  Here, a description of the data exporter's business or organisation type should be set out. The activities of the exporter's business must also be described, insofar as they are relevant to the transfer at hand.
  So, for example, the exporter's business might be described as "Manufacturer of motor components". The activities of the business to which the transfer is relevant must also be described. If, for example, the business uses an occupational health insurance provider based in the UK for its employees, then its activities as they relate to the transfer might be described as "administration of insurance schemes, including the administration of health insurance business by an insurance firm."
- *Heading #2* – "**Data Importer**"
  Here, a description of the data importer's business or organisation type must be set out, along with a description of the activities of the exporter's business, as they relate to the transfer.
  Building on the example under Heading #1, the importer's business might be described as "Insurance Services Provider", and its relevant activities as "insurance administration including the administration of life, health and other insurance business."
- *Heading #3* – "**Data Subjects**"
  Here, the parties must identify the categories of data subjects to whom the transferred data relates. Sticking with the example used above, a description along the following lines might be used: "Direct employees, past and present."
- *Heading #4* – "**Categories of Data**"
  Here, the parties must describe the categories of data to be transferred. In the example we're using, this might read something like this: "personal, financial and employment related data as required for the administration of the data exporter's occupational health insurance scheme, and the participation of the data exporter's employees in that scheme."
- *Heading #5* – "**Special categories of data**"
  Here, any special categories of data (i.e. what was previously described as "sensitive personal data") must be identified. In our example, this could include, for example, health-related data that may be need to be processed in the context of an employee's participation in the data exporter's occupational health insurance scheme.
- *Heading #6* – "**Processing Operations**"
  Here, the parties must provide details of what it is they will be doing with the data that is to be transferred, i.e. the processing operations and activities to which the data will be subject. This might include a description

along the following lines: "receiving data, and accessing, retrieving, and recording same."

Appendix 2

In **Appendix 2** the parties must describe the technical and organisational security measures implemented by the importer to protect data subjects' personal data in accordance with Clauses 4 and 5. The description to be inserted here will necessarily depend on (for example) *what* data is being transferred and *how* it is being processed. The kinds of things that might be described here might include things like:

- Security elements of the IT systems deployed by the importer, e.g. the use of encryption;
- Details of the controls in place to limit (and regulate) access to the data;
- The use of logging mechanisms to verify whether and by whom the data has been accessed, used and/or disclosed.

Conclusion

It is important to bear in mind that SCCs (and indeed any of the other mechanisms used to facilitate the lawful transfer of data out of the EU/EEA) are not an end in themselves.

Care is required to ensure that, operationally, transfers are conducted and managed in a way that ensures that personal data is at all times protected to the level contemplated by the GDPR and that the obligations assumed by the parties under the terms of their SCCs contract are in fact discharged *in practice*.

Like all other elements of the data processing arrangements of a business, planning is required to ensure compliance with GDPR requirements generally.