



External Data Transfer Policy

External Data Transfer Policy

INTRODUCTION

As part of our daily business, all employees interact with personal data and may be required to transfer personal data to external parties for varying purposes. This policy provides guidelines on the transfer of personal data by, on behalf of or in connection with The DPO Centre Ltd (henceforth referred to as “the DPO Centre”, “the Company” or “we”).

All employees, agents and contractors of the DPO Centre are required to act in accordance with this policy at all time. The DPO Centre aims to ensure that this policy is well understood and therefore should you have any questions in relation to this policy and how it applies to you please contact Dennis Ley (HWDennis.Ley@holmwoodschool.ogr.uk or 01642 819 157)

DEFINITION OF TERMS USED WITHIN THIS POLICY

- a. Any reference to “Article” or “Articles” is a reference to an Article or Articles of the General Data Protection Regulation (Regulation (EU) 2016 679), (henceforth referred to as “GDPR”).
- b. The terms ‘personal data’, ‘data subject’, ‘processing’, ‘pseudonymisation’, ‘controller’, ‘processor’, ‘recipient’, ‘third party’, ‘consent’, ‘international organisation’, have the meanings set out in Article 4.

GENERAL PRINCIPLES FOR DATA TRANSFER

Personal data must be handled in line with the data protection principles set out in Article 5 of the GDPR. When transferring data to another person or legal entity, these principles must be established and evident in the transfer. Therefore, whenever data is being transferred, particularly to external recipients The DPO Centre, its employees, agents and contractors must observe the following points in particular:

- a. Any transfer of personal data must be lawful and will only be considered so to the extent that at least one of the legal basis set out in Article 6 of the GDPR applies to the transfer. In the event that a legal basis does not exist for an intended transfer of personal data, such transfer should not take place. It is therefore essential that a defined purpose, consistent with the purposes for which the relevant data was collected and otherwise processed is established for any such transfer.

The transfer of personal data to any parties who are not contractually associated with the DPO Centre at the time of the transfer is strictly prohibited and any employee, agent or contractor found sharing data with any disassociated third parties will face disciplinary actions which may include dismissal.

- b. Any transfers of personal data must be fair and transparent. Data subjects should be informed of any intended transfer of their personal data and the purpose(s) of the transfer prior to the transfer taking place in accordance with Articles 12 to 15.

The DPO Centre aims to ensure that any possible transfers of personal data are detailed within any privacy or other notices that have been made available to the data subjects to whom the personal data relates. If no such notices have been made available, the relevant data subjects they should be informed prior to the transfer.

- c. It is the responsibility of the DPO Centre, its employees, agents and contractors to ensure that any personal data transferred is accurate and limited to data necessary for the fulfilment of the established purposes. Any data that is transferred and later found to be incorrect should be rectified without undue delay.

TRANSFER OF SPECIAL CATEGORY DATA

Special categories of personal data is defined within Article 9 of the GDPR and includes:

- Racial or ethnic origin
- Political opinion
- Religious and philosophical beliefs
- Trade union membership
- Genetic or biometric data which uniquely identifies a person
- Health data
- Data concerning a person's sex life or sexual orientation

The DPO Centre prohibits the external transfer of special category data. Any employee, agent or contractor of the DPO Centre who is asked to transfer any special category data or believes they are required to make such transfer for the fulfilment of a task performed on behalf of the DPO Centre must consult their line manager.

SECURE TRANSFER OF PERSONAL DATA

All employees, agents and contractors of the DPO Centre are required to ensure that personal data is transferred securely. Where any personal data is shared via email, encryption of such emails is mandatory. Personal data transferred to external recipients should be done via a password protected file sharing portal.

TRANSFERS WITHIN THE EEA

Any transfer of personal data to parties within the EEA must comply with the above provision. Prior to any such transfer taking place the DPO Centre, its employees, agents and contractors must ensure that written agreements are in place which cover the transfer of data and ensure the recipient offers appropriate confidentiality, information security and data protection undertakings.

TRANSFERS OUTSIDE THE EEA

Transfers of personal data to recipients located outside the EEA (to a third country) are subject to specific requirements and can only take place if any of the conditions set out in Articles 45 – 47 can be applied to the transfer.

Such transfers include, without limitation transfers to an international organisation which has locations in both a third country and the EEA. A transfer to an international organisation with locations within the EEA is still considered an international transfer of personal data for the purposes for the GDPR and this policy and is subject to specific requirements.

Due to the additional requirements applicable to international transfers of personal data, all such transfers must be authorised by an employee of manager level and above. Such authorising employees are responsible for checking that the transfer is permissible based on the existence of one of the following:

- a. The third country or international organisation has received an adequacy decision from the European Commission stating that the third country or international organisation ensures an adequate level of data protection.

If the third country or international organisation is subject to an adequacy decisions, an employee of manager level or above may authorise the transfer subject to the requirement detailed above being met.

- b. In the absence of an adequacy decision, a transfer may be authorised where appropriate standard contractual clauses have been agreed between the parties to the transfer.

For transfers to the United States of America, the transfer may be authorised without the standard contractual clauses where the recipient can provide evidence of a EU-US Privacy Shield certification. In such cases, it is within the manager's discretion to require standard contractual clauses to be agreed as an additional safeguard.

- c. International transfers of personal data within a group of undertakings or a group of enterprises engaged in a joint economic activity, of which the DPO Centre is a member, may be authorised where approved binding corporate rules exists as set out in Article 47 of the GDPR.
- d. In the absence of a. to c. above, the general prohibition on transfers of personal data to third countries can be derogated from in certain specific situations. A transfer, or set of transfers, may be made where the transfer is:

- made with the data subject's informed consent which is obtained having informed the data subject of the possible risk associated with such transfer due to the absence of an adequacy decision and appropriate safeguards;
- necessary for the performance of a contract between the data subject and the recipient or for pre-contractual steps taken at the data subject's request;
- necessary for the performance of a contract made in the interests of the data subject between the controller and another person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defence of legal claims;
- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- made from a register which, by law, is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).