INCLUSIVE SKATING

Advice Note on Data Transfers Outside of the EEA

Transfers of personal data to "third countries" (i.e. outside of the European Economic Area) continue to be restricted under the General Data Protection Regulation (**GDPR**) with the current requirements under the Data Protection Act 1998 ("**DPA**") broadly remaining in place with some improvements.

What constitutes a data transfer?

Under the DPA, the prohibition on data exports only applied to an actual transfer of personal data to a country or territory outside the EEA (**third country**). It did not apply if the data simply passed through a third country in transit to a final destination in the EEA, unless some substantive processing took place in that third country en route.

The general principle for data transfers under the GDPR however applies to data "*which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation*" (Article 44, GDPR).

Therefore a cross-border transfer will be deemed to have occurred if any personal data can be accessed in a third country outside the EEA e.g. where personal data has been uploaded into a shared database or the internet with the intention that it should be accessed in a third country.

For example, *consider whether you use a centralised database or HR system that is hosted by a third party service provider outside of the EEA or whether you send information about a player to a third country such as Australia for the purposes of organising accommodation for an event. If you do, cross-border transfers will be deemed to have occurred.*

These restrictions and rules mean that you need to be very aware of where personal data is going, particularly if you are using Cloud-based services or products. If your

data is being transferred outside the EEA, be careful that you have not left your organisation at risk.

What does this mean for your organisation?

You may only transfer personal data to a third country or to an international organisation (i.e. *an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries*), as long as **either**:

- the European Commission has decided that the third country, a territory or one or more specific sectors within that third country, or the international organisation ensures an ***adequate level of protection*** (Article 45(1), GDPR); **or**
- the controller or processor has:
    - provided ***appropriate safeguards*** in accordance with Article 46(2) of the GDPR (see below for a list of these); and
    - enforceable data subject rights and effective legal remedies for data subjects are available.

Which countries have been approved as providing an 'adequate level of protection' by the EU Commission?

The existing list of countries which have previously been approved by the Commission will remain in force, namely: ***Andorra, Argentina, Canada (where 'the Personal Information Protection and Electronic Documents Act' applies), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.*** *If your personal data is being transferred to organisations within these countries, you do not need to apply any further safeguards.*

No general finding of adequacy has been made in relation to the **United States**, but on 12 July 2016, the European Commission formally adopted a decision confirming the adequacy of the EU-U.S. Privacy Shield.

US organisations may therefore self-certify to the standards set out in the Privacy Shield from 1 August 2016. As the Commission's decision establishing the Privacy Shield was originally adopted pursuant to Article 25(6) of the Data Protection Directive, it will continue to apply after the GDPR comes into force in May 2018.

The Privacy Shield is one of a number of mechanisms for transfers of personal data to the US. A good first step is to see whether the US organisations you transfer personal data are part of the Privacy Shield scheme. If the company you want to transfer data to is not certified, you cannot rely on the Privacy Shield and *must* rely on another safeguard.

What constitutes appropriate safeguards?

In the absence of a Commission adequacy decision, *(i.e. if you transfer data to a country not on the above approved list or to a US organisation that is not part of the Privacy Shield scheme)* you may still transfer personal data to a third country or an international organisation as long as you have implemented appropriate safeguards such as:

- standard data protection clauses in the form of template transfer clauses either adopted by a supervisory authority and approved by the Commission or adopted by the EU Commission ***(This is likely to be the set of safeguards most relevant to UK-based sport organisations. Please see standard contractual clauses in the Data Transfer Agreement – Outside the EEA);***
- a legally binding agreement between public authorities or bodies;

- binding corporate rules (*where a transfer is carried out by a UK-established company to other members of its group in different jurisdictions, the transfer will comply with the GDPR if it is governed by a set of legally enforceable corporate rules) that have been approved by the Information Commissioner*);
- transfers will be permitted where an approved code of conduct (*based on the new scheme in Article 40 of the GDPR*) or an approved certification mechanism (*based on the new scheme in Article 42 of the GDPR*) is used, provided that binding and enforceable commitments are made by the controller or processor in the third country to apply the appropriate safeguards, including as regards the data subjects' rights;
- contractual clauses authorised by the competent supervisory authority *(controllers and processors are now also permitted to transfer personal data to a third country on the basis of contractual clauses agreed between them and the processor, controller or recipient of the data in the third country. Those types of clauses are likely to relate to one-off transfers or to repeated transfers between the same parties and are however subject to the authorisation from the competent national supervisory authority and so given the administrative burden that the authorisation process will on parties wishing to rely on those clauses, it is likely that this approach will only be commercially viable for large scale controllers and processors); or*
- provisions inserted in to administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Are there any exceptions?

In the absence of a Commission adequacy decision or the establishment of appropriate safeguards (*see above),* you may transfer personal data to a third country or an international organisation if one of the following conditions applies:

- The individuals concerned have ***explicitly consented*** to the proposed transfer, after having been informed of the possible risks of that transfer that arise from the absence of an adequacy decision or appropriate safeguards
- The transfer is necessary:
    - for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request. A transfer will be "necessary" in these circumstances where it is required to perform a contract (such as where an organisation passes names and addresses to its overseas manufacturer of any products it is selling for the purpose of delivery), but not where it is due to the structure of the data controller's business (for example, where a controller chooses to locate any of its data processing operations outside the UK);
    - for the performance of a contract between the controller and a third party that is concluded in the interest of the data subject;
    - for important reasons of public interest e.g. in cases of international data exchange between tax or customs administrations, between financial supervisory authorities or for public health in order to reduce or eliminate doping in sport*;*
    - for the establishment, exercise or defence of legal claims; or
    - to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent (that is, a life-or-death situation). A transfer justified under this condition could

include the transfer of medical records where the individual has been in a serious accident abroad.

- The transfer is made from a register which under UK or EU 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).
- There is also a new (limited) derogation for non-repetitive transfers involving a limited number of data subjects where the transfer is necessary for compelling legitimate interests of the controller (which are not overridden by the interests or rights of the data subject) and where the controller has assessed (and documented) all the circumstances surrounding the data transfer and concluded there is adequacy. The controller must inform the supervisory authority and the data subjects when relying on this derogation so it is likely to have limited application.

Enforcement

Sending personal data to a third party in a country outside the EEA that does not provide the data subject with an adequate level of data protection is a breach of the GDPR's cross-border transfer provision that will be subject to the full enforcement powers of the national supervisory authorities.

The GDPR grants supervisory authorities significantly enhanced powers to enforce its provisions and to obtain compensation for its breach. Among other things, supervisory authorities are granted:

- Several investigative, corrective and authorisation and advisory powers *(Article 58, GDPR); and*
- The power to impose administrative fines on controllers and processors *(Article 83, GDPR).*

Data subjects have a right to lodge a complaint with the competent national supervisory authority and to an effective judicial remedy against a national supervisory authority and against infringing controllers and processors *(Articles 78 and 79, GDPR).*