Brexit: Data Protection

All sporting organisations are affected by 'Data Protection' in some shape or form, whether that's because of the data they collect in respect of their volunteers and staff, the performance analysis of their athletes, marketing to their members or the data they receive to support their integrity and regulatory functions in respect of anti-doping and betting for example, each organisation must currently comply with the General Data Protection Regulation ("**GDPR**") and the Data Protection Act 2018. We have all seen the headlines regarding the potential fines that could be imposed if you fail to comply with the requirements of GDPR, but perhaps of more a concern for the sports and recreation sector is that under the Code for Sports Governance, sports organisations risk losing their funding for non-compliance with applicable regulations such as GDPR.

But, "surely, if we are leaving the EU, none of this matter will matter anymore?" Unfortunately- or fortunately- depending on which side of the data protection fence you sit, this is not the case and this note will aim to explain why and to give you an overview of the implications of Brexit for data protection law in the UK for the sport and recreation sector should we leave the EU with no deal.

It is not intended to provide legal advice and for further guidance please check out the ICO's website at https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-and-brexit-for-small-organisations/.

Do we still have to comply with GDPR if we leave the EU?

GDPR is an EU Regulation and, therefore, it will no longer apply to the UK if and when we leave the EU regardless of whether we leave with a deal or not. Therefore, strictly you will not have to comply with it *(although GDPR will continue to apply in the UK during any transition period in the event we leave with a deal -see note below).* However, new regulations have been passed by UK Parliament, which essentially will make technical amendments to the GDPR, by essentially merging the Data Protection Act 2018 (which will continue to apply in the UK once we leave the EU) and the GDPR so that it works in a UK-only context from the day we leave. In practice, this means therefore that there will be little change to the core data protection principles, rights and obligations found in the GDPR so for now at least organisations should continue to comply with GDPR as they have done before.

What does this mean practically for our organisation?

We will come on to what this all means for ***data transfers*** to and from the EU below, but first:

- If your organisation is operating in another member state of the EEA, not just the UK, you will need to comply with both the GDPR and UK GDPR after Brexit.

- If your organisation has offices, branches or other establishments in the EEA, its European activities will be covered by GDPR, even after Brexit.

- If your organisation is only based in the UK but offers products or services to individuals in the EEA or monitors the behaviour of individuals in the EEA, you will still need to comply with GDPR in relation to these activities as well as UK GDPR. For example, if your organisation's website is likely to attract individuals based in the EU and uses tools to monitor and analyse its users' preferences, you may well be caught by GDPR.

What if we leave the EU with a deal in place?

- In the event of a deal with the EU, the UK and EU will have negotiated the 'Withdrawal Agreement' as a basis for securing a smooth transition in the immediate aftermath of the UK's formal departure from the EU. The Agreement provides for a transition period during

which the UK will remain subject to all EU laws (other than those expressly excluded within the Withdrawal Agreement). This means that during this transition period, GDPR will continue to apply in the UK and organisations won't need to take any immediate action.

- The GDPR shall also continue to apply within the UK as EU law after the transition period, insofar as any EU originating personal data continue to be processed within the UK post-transition, where the relevant data commenced before the end of the transition. This is designed to protect EU residents' privacy rights to ensure that EU resident data collected within the UK during the transition period does not lose GDPR protection just because transition ends, e.g. where a French athlete and his/her family members have relocated to the UK to help further the athlete's career in a particular sport. This protective provision will fall away if the UK secures an EU adequacy decision (see below) at any time.

- At the end of the transition period, the default position would be the same as for a no-deal Brexit above, but there may be time for further developments since this note was prepared.

Will Brexit cause us any issues in transferring data in and out of the EU?

Transfers outbound from the UK

- The UK will be a "third country" once we leave the EU with or without a deal. The UK Government has confirmed that following Brexit it does not intend to apply these restrictions on transfers of personal data from the UK to the EEA. This is because outbound international transfers of personal data will be subject to the UK GDPR. The DP Brexit Regulations transitionally recognise all EEA countries as "adequate", so permitting data transfers to these countries to continue.

- Therefore, UK organisations will continue to be able to send personal data to organisations in the EEA completely unrestricted, so you can continue as before e.g. where you use a centralised database that stores data in the EEA or where you send information about an athlete to, say, Germany for the purposes of organising accommodation for an event. UK organisations will also be able to continue to rely on the EU/US Privacy Shield scheme to send personal data to registered entities in the US, but only where the US entity has updated its privacy notice to expressly extend protection to transfers from the UK. These are intended to be temporary measures, and in time the UK is expected to conduct its own adequacy assessments (including of EU member states).

Transfers inbound to the UK

- The EU has not, however, granted similar modification in respect of transfers to the UK. Following Brexit, transfers of personal data from the EEA to the UK will be restricted and this is where it gets a little more difficult.

- This means than an organisation will only be able to transfer personal data **inbound** to the UK as long as either:

    - the European Commission has decided that the UK ensures an adequate level of protection (an "**Adequacy Decision**"); or
    - the organisation has provided appropriate safeguards for the transfer (e.g. for many organisations the best approach will be to adopt the Standard Contractual Clauses

(**SCCs**) which have been approved by the EU as a legal basis to safeguard the transfer of personal data to third countries which will include the UK after Brexit).

- Therefore, if you are receipt of personal data from third parties based in the EU, perhaps you are a sports federation that relies on the sharing of suspicious sport betting data for the prevention of fraud in the gambling market, something that is often cross-border- the lack of a clear route for these sorts of transfers may complicate things. However, it shouldn't have to. Whilst every case is different there is no reason that the third organisation in the EEA can't use SCCs. Whilst it is the EEA data controller of the personal data which must comply with the GDPR rules, organisations in the UK who want to receive the data, may want to assist those senders in complying to ensure the continuous flow of data.

- In the absence of an Adequacy Decision or the establishment of appropriate safeguards, organisations may also transfer personal data to the UK or an international organisation outside of the EU if the transfer falls within one of the narrowly construed derogations set out in GDPR, including express consent from the data subject or where the transfer is necessarily to perform a contract (***See GDPR Toolkit for further guidance).***

- It is important to be however aware that SCCs cannot be used to safeguard transfers between an EU-based processor and a UK-based controller (i.e. where a UK controller hosts personal data with an EU processor) so there is a potential difficulty where you have EU based organisations or individuals processing personal data on your behalf, e.g. external examiners based in the EU who have been instructed to assess a participant's performance on a training course or event abroad or a safeguarding platform provider based in Ireland to give a couple of examples.

- The UK hopes to secure an 'adequacy' finding from the EU that will remove the need for SCCs or other specific safeguards between the UK and the EU. The EU has indicated it's prepared to consider this, but not until after Brexit, regardless of whether we leave with a deal or not. An Adequacy Decision is unlikely within the first 12 months following exit-day so, in the meantime, this is a known area of risk, which is one you should be alive to and manage accordingly in the event of a no deal, where data repatriation from the EU is not a realistic or cost-efficient option for your organisation.

What can we do now to plan ahead?

- Update references in all governance records, contracts and privacy notices to the EU/EEA to reflect the post-Brexit position of the UK being outside the EU. This may require changes to:
    - Records of processing activities, insofar as these are impacted by Brexit;
    - Privacy Notices. These are likely to be minor, for example, to update references to relevant laws (such as changing the GDPR to the UK GDPR) and to include transfers from the UK to the EU. **These changes would need to be made at the time of Brexit or as soon as possible afterwards**;
    - Data Protection Impact Assessments may need to be updated if they refer to a transfer which becomes a transfer to a 'third country' on exit-date; and
    - Contracts with third parties, if they include specific reference to the GDPR, EEA or anticipate a data transfer between the EU and the UK.

Is there anything else we need to consider?

- If your organisation will be subject to regulatory responsibilities under both GDPR and UK GDPR (as explained above), this may result in additional compliance requirements:
    - You may need to appoint a separate data protection officer (DPO) for both the UK and EU;
    - You may need to nominate a new lead supervisory authority in the EU as well as registering with the ICO for processing activities in the UK;
    - You many need to appoint a local representative in the EU/UK, where you are processing data from outside the jurisdiction; and
    - Whilst the ICO still intends to co-operate and collaborate with other EU supervisory authorities and are expected to act proportionately, in particular on data breaches, it is possible that multinational organisations could face both EU and UK fines or action for the same breach.

There are good grounds for expecting a reasoned and pragmatic approach from the ICO and the UK government when we move into the unchartered UK GDPR territory and each business has its own different data protection requirements, but you should take focused advice from a data protection specialist if you are concerned. If you have any questions, Gateley Legal's Data Protection team will be happy to help.

.