Safeguarding in Sport: Considering Subject Access Requests

14 October 2021

SPORT RESOLUTIONS

LEWIS SILKIN

Safeguarding in Sport: Considering Subject Access Requests

Speakers

Alexander Milner-Smith, Co-Head of Lewis Silkin's Data & Privacy Group

Sean Illing, Senior Associate

LEWIS SILKIN

What are we going to talk about?

- How to consider data sharing in the safeguarding case management context
- Intro to SARS
- Technicality of the legislation
- Issues to consider when dealing with safeguarding data about children or adults at risk
- How and when can safeguarding data be lawfully shared without consent
- Issues to consider when creating a policy or protocol to guide your responses
- Tactics & Practical Tips

Questions throughout please!

Key Grammar

Key Definitions

Article 4 of the GDPR defines some key terms relating to SARs, it specifies that:

- '**Personal Data**' means any information relating to an identified or identifiable natural person (a '**Data Subject**').
- Relevant *'Information'* – essentially e-data and information held in manual filing systems (Article 2(1) GDPR)
- When is a person '*identified'* or *'identifiable*'?
  - Includes direct and indirect identification, in particular by reference to an identifier: not just names but also ID number, online identifiers such as IP addresses, location data, or factors physiological, genetic, mental, economic, cultural factors or social identity specific to the individual).
- What does information *'relating to'* a person mean?

Key Grammar cont.

- A '**Data Controller**' (Article 4) – a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
  - concept of autonomous, self-directing control central to definition
  - agents working for a principal can also be controllers (e.g. lawyers, private investigators)
- A '**Data Processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

How to consider sharing in the safeguarding case management context

- Data may need to be shared – e.g. with the police, with a regulatory body, or with an investigator. Consider the relationship – controller or processor?
- Consider what the data subject has been told – has the privacy policy set out the purposes for the processing, and who personal data might be shared with?
- Consider the obligations of both parties – has a data processing agreement been entered into that ensures the parties are contractually obliged to treat the data appropriately?

What is a SAR? (Briefly)

- A **Subject Access Request (SAR)** gives an individual (data subject) the right to request access to any and all **personal data** that a controller processes about them. It also allows the **data subject** the right to access other supplementary information.
- An individual can make a SAR to you or any part of your organisation, **verbally or in writing**. It does not have to be made to a specific person or at a specific contact point.
- A request does not have to include the phrase ‘subject access request’ or “Article 15 of the GDPR”. So it’s important that **you know how to recognise when a SAR has been made**.
- It’s good practice to have a policy for **recording details of the requests** you receive, particularly those made by telephone or in person.

Context of SARs

- Now routinely used in disputes
- Potentially **significant burdens** for controller/**diversion of resources**
- Commonly used as a **tactical weapon** (to obtain early disclosure or gain leverage in settlement negotiations)
  - Importantly **motive of requester** generally not a reason for refusing (***Dawson-Damer v Taylor Wessing***)
- Getting it wrong can result in both:
  - **legal action** (brought by the requester *or* affected third party individuals) and
  - **regulatory action** (by the ICO)

What is a SAR?

Article 15 GDPR (bites on controllers only)

- Affords right of **access to personal data being processed by the controller (including a copy of that data)**, or confirmation that no personal data are being processed **plus** the following information:
  - the purposes of the processing;
  - the categories of personal data concerned;
  - **the recipients or categories of recipient** to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
  - where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
  - the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

What is a SAR?

Article 15 GDPR - Right of access by the data subject (cont.)

- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- Where personal data are transferred to a non-EU country or to an international organisation, the data subject shall have the right to be informed of the safeguards taken relating to the transfer.

- **(Subject to Brexit)** – Right of subject access is a **fundamental right** guaranteed by Article 8 of the EU Charter of Fundamental Rights.

Additional relevant rules in GDPR

Article 12 - Transparent information, communication and exercising the rights of the data subject

- Duty on controller to take appropriate measures to provide SAR communications in **a concise, transparent, intelligible and easily accessible form, using clear and plain language**.
- The controller shall not refuse to act on a SAR, unless the controller demonstrates that it is **not in a position to identify the data subject**.
- If the controller has reasonable **doubts about the requester's identity**, the controller may request additional information necessary to confirm their identity.
- The controller shall provide the requester with information on action taken on a SAR **without undue delay and in any event within one month** of receipt of the request. That period may be extended by **two further months** where necessary, taking **into account the complexity and number of the requests**.

Additional relevant rules in GDPR

Article 12 - Transparent information, communication and exercising the rights of the data subject (cont.)

- The controller shall inform the data subject of any such extension **within one month of receipt of the request, together with the reasons for the delay**.
- Where the **request is made by electronic means**, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
- Where a request is **manifestly unfounded or excessive, in particular because of its repetitive character**, the controller may either
  - charge a **reasonable fee** (taking into account the administrative costs of providing the information) or
  - **refuse to act** on the request

  Outside these exceptional circumstances no fees may be imposed by the controller

Issues to consider when dealing with safeguarding data about children or adults at risk

- Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If the request is from a child and you are confident they can understand their rights, you should usually respond directly to the child. You may, however, allow the parent or guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child. If a child is competent, they may authorise someone else, other than a parent or guardian, to make a SAR on their behalf.
- Consider the context of the request and ensure that, whatever decision you make, you support that decision with written evidence
- Where children's data arises in a third party's DSAR – consider whether it would be reasonable to disclose it (we will come onto third party issues).

Do we have to provide everything?

- So, a SAR has been made. **Do you have to provide everything?**
  - Simple answer is **no**, you do not have to provide everything.
- There are certain limits and exemptions put in place that allow you the right to not provide certain documents to the data subject. Some of those are;
  - Specific exemptions provided under the **Data Privacy Act 2018**
  - Proportionality limits under general EU principles but also ICO guidance and case law
  - Duty to provide copy data applies only to ‘data’ not to ‘documents’.

SAR Exemptions

- **Article 23 GDPR** provides that the rights afforded under the GDPR (including SAR rights) may be subject to restrictions so as to protect a variety of rights and interests
- Article 23 has been implemented in s.15 Data Protection Act 2018 which provides for **exemptions** (in the DPA Schedules 2, 3 and 4)
  - broadly speaking, contains the same exemptions that were allowed under the old regime, but with some important changes
- **A key exemption in the SAR context: the mixed data exemption**
  - falls to be considered where requester's data inextricably mixed with third party personal data (engages third party privacy/data protection rights)
  - (broadly) a controller does not have to disclose mixed data does not need to be disclosed unless:
    - the third party has consented or
    - it is reasonable to provide such data without consent (balancing the competing rights and interests)

SAR Exemptions in the Data Protection Act 2018

- **Other key exemptions**

  - **Legal privilege** – controllers do not have to disclose data which is covered by legal professional privilege (**legal advice and litigation privilege**)

  - **Lawyers' confidentiality** - Legal advisers do not have to disclose information which they hold under a duty of confidentiality to their client

    - On the face of 19(b) SAR rights do not trump client confidentiality

    - Always remember how wide duty of confidence actually is (***Phipps et al***)

SAR Exemptions in the Data Protection Act 2018

- **Confidential references** – employers do not have to provide the data subject access to references they have confidentially given (or received) in relation to their employment.
- **Management information** – personal data which relates to management forecasting or planning is exempt from right of access to the extent that complying with the SAR would be likely to prejudice the business activity of an organisation.
- **Settlement negotiations** – data subjects are not entitled to personal data which consists of a record of an employer's intentions in respect of settlement discussions to which they are a party.

- Note also exemptions re prejudice to **criminal law enforcement** and taxation, discharge of **functions to protect the public** and **regulatory functions (e.g. section 26 of the Children Act relating to Local Authority reviews)**.

- Note all the exemptions must be **construed and applied limitatively** because of the impact on fundamental rights

SAR Exemptions in the Data Protection Act 2018

PART 5

CHILD ABUSE DATA

Exemption from Article 15 of the GDPR: child abuse data

21 (1) This paragraph applies where a request for child abuse data is made in exercise of a power conferred by an enactment or rule of law and—

(a) the data subject is an individual aged under 18 and the person making the request has parental responsibility for the data subject, or

(b) the data subject is incapable of managing his or her own affairs and the person making the request has been appointed by a court to manage those affairs.

(2) Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) do not apply to child abuse data to the extent that the application of that provision would not be in the best interests of the data subject.

(3) "Child abuse data" is personal data consisting of information as to whether the data subject is or has been the subject of, or may be at risk of, child abuse.

(4) For this purpose, "child abuse" includes physical injury (other than accidental injury) to, and physical and emotional neglect, ill-treatment and sexual abuse of, an individual aged under 18.

(5) This paragraph does not apply in relation to Scotland.

Proportionality limits and tactics

ICO Code on Subject Access (still relevant)

- General comment
  - *You should be prepared to make extensive efforts to find and retrieve the requested information. Even so, you are not required to do things that would be **unreasonable or disproportionate** to the importance of providing subject access to the information. Any decision on these matters should reflect the fact that the right of subject access is fundamental to data protection.*
- ICO comment on case law
  - *The court also made it clear that in assessing whether complying with a SAR **would involve disproportionate** effort under section 8(2)(a) you may take into account difficulties **which occur throughout the process of complying with the request**, including any difficulties you encounter in finding the requested information.*
  - ***This approach accords with the concept of proportionality in EU law, on which the DPA is based**. When responding to SARs, we expect you to evaluate the particular circumstances of each request, balancing any difficulties involved in complying with the request against the benefits the information might bring to the data subject, whilst bearing in mind the fundamental nature of the right of subject access.*

Proportionality limits and tactics

- Reliance on the **'manifestly unreasonable or excessive'** requests exemption:
  - Remains **unclear what 'manifestly unreasonable' or 'excessive' means**
    - likely to be a high threshold
  - Article 12 provides that **controllers shall bear the burden** of demonstrating the manifestly unfounded or excessive character of the request.
    - May be challenging to discharge this burden in practice
    - Important to keep records of your exploratory assessment of the issue (including the extent to which you conducted searches to assess whether the request was excessive).

How and when can safeguarding data be lawfully shared without consent?

- Article 6 – legal obligation or legitimate interests?
- And is the data ‘special data’?
- In which case an Article 9 condition will also need to be relied upon:
  - Substantial public interest?
  - Establishment, exercise or defence of legal claims?

How to handle a SAR

- Basic steps/questions
  - **ID?** Have you checked the data subject is who they say they are?
  - **Start a high level search**. This may run to hundreds of thousands of documents.
  - **Acknowledge the SAR**. Would you regard this request as vanilla or complex? Is this request manifestly excessive?
  - Commence **further correspondence** with the data subject to narrow down the scope?
  - **Hone the searches**. Will key search terms in conjunction with the data subject's name narrow the number of documents
  - **Review** - What are your review parameters? Are you going to release third party data that already known without redaction? What is your risk tolerance? How are you applying exemptions?
  - **Cover letter** setting out all of the information that is required by Article 15 and provision of personal data.
  - Prepare to follow up on any **complaints** about your handling of the process.
- Think tactically at all times:
  - What is Data Subject trying to achieve?
  - Who is my audience for correspondence?

Issues to consider when creating a policy or protocol to guide your responses

- DSARs are like snowflakes – every one is unique
- There are certain parts of a DSAR that will be common to each one:
  - The one/three month deadline for responding; and
  - The fact that manifestly excessive DSARs can be refused.
- However, there will also be key differences:
  - The media that are searched;
  - The data that is selected to review; and
  - The approach to redactions.
- The key to a useful policy is to demonstrate to readers the importance of compliance, but not making it so restrictive as to prevent responding to DSARs in the most practical and useful way.

Top cases run through (all pre-GDPR)

- ***Dawson-Damer v Taylor Wessing [2017] EWCA Civ 74***
  - TW not entitled to rely on **proportionality arguments which were not evidence-based**. TW's **failure to test its assumptions** on proportionality by conducting an assessment of the data it held was fatal to its case
  - The **SAR regime does not recognise a motive test**. It was clearly designed to protect interests going beyond privacy rights.
- ***Ittihadieh v Cheyne Gardens/Deer v Oxford Uni [2017] EWCA Civ 121***
  - **Searches** – The requirement is for **reasonable and proportionate** searches not to leave every stone unturned [103]
- ***B v General Medical Council [2018] EWCA Civ 1497***
  - Court should seek to review not second guess the controller's decision on how to strike the balance between disclosing data to the data subject and protecting third party data.

Courts vs. ICO Enforcement – what are the options?

- Requesters at liberty to bring **claim** before the courts whilst also seeking an **assessment** from ICO.
  - Entirely common for requesters to do both in the hope of obtaining ICO assessment that renders court action a fait accompli
- Alternatively, requesters (who do not want to incur legal costs) can invite ICO to take enforcement action
  - However, generally not an area in which ICO has shown an appetite to take enforcement action
- That said, important to bear in mind that breaches can in principle expose the controller to:
  - Court claims for **injunctive relief** (under Art 79 GDPR) and/or **damages** (under Article 82 GDPR), along with the risk of potential adverse **costs** orders (as in ***Holyoake***), as well as **regulatory action** by the ICO, including in serious cases the risk of monetary **penalties**

Practical tips

- **Early constructive engagement with the requester** is crucial
  - They don't have to engage on the issues of scope/search terms but it may help you on proportionality if they don't.
- Adopt a **careful, considered approach** to the devising of search protocols and weeding exercise
- **Avoid making untested, self-serving assumptions** about what you've got or whether data is exempt
- Try to **demonstrate a committed approach**
  - Compare *Dawson-Damer* and *Gaines-Cooper*
- **Constructive engagement with the ICO** is key

Record keeping

- Data subjects will often complain about the approach that has been taken to their request. Best practice is to keep a record of the data that has been supplied, the approach taken, and any correspondence in case of an investigation by the ICO, or a court claim.
- It can also be useful to keep a record of where DSARs have originated in order to spot patterns and try to nip issues in the bud.
- Keeping a record will also demonstrate compliance with the Article 24 obligation to demonstrate that processing is taking place in accordance with the UK GDPR

Questions?

Contact Details

Alexander Milner-Smith
Co-Head Data and Privacy
Alexander.Milner-Smith@lewisilkin.com
020 7074 8196

Sean Illing
Senior Associate, Data & Privacy
Sean.Illing@lewissilkin.com
020 7074 8272