Guest columnist

OLIVIA WHITCROFT

"Our customer services rep called them a twerp – can I withhold this?"

A customer asks you for access to their personal data. How do you prove they are who they say they are? And how much information do you provide?

Since the start of the summer, a lucky dip of legal queries has landed on my desk. From subject access requests to restrictive covenants in technology consultancy agreements, and onwards to software development contracts between multiple parties. Data protection queries requiring analysis of relationships between controllers, joint controllers and processors. And a request for an innovative contract with a social media influencer.

I would love to write about all of these, but I suspect there are other exciting matters to cover in this edition of *PC Pro*. So I thought I would pull out a couple of interesting technology-related queries on the first topic: subject access requests.

Subject access requests

Under Article 15 UK GDPR, an individual has a right of access to their personal data held by organisations. A request to exercise this right is often called a "subject access request" (SAR).

When I am consulted in relation to a SAR, the question is often whether particular information falls within the meaning of "personal data" or whether an exemption can be applied to withhold some data from the response.

Some themes come up a lot ("Do I have to provide every email that mentions them over the past 20 years?"; "Our customer services rep called them a twerp – can I withhold this?"). But the queries discussed here are more unusual, and bring up lesser-studied aspects of the rules.

Online identifiers

A company received a request from an individual to access information associated with an internet protocol (IP) address, which the requestor said was assigned to their computer. The question posed to me by the company was: do we need to provide this data?

Olivia is principal of the law firm OBEP, which specialises in technology contracts, IP and data protection
@ObepOlivia

As mentioned, a person has a right of access to personal data. Personal data means any information relating to an identified or identifiable individual, and someone can be identified by an "online identifier" (Article 4(1) UK GDPR). Recital 30 includes IP addresses and cookie identifiers as examples of online identifiers. So, in theory, information associated with an IP address (such as logs of access to a website, or behavioural advertising profiles) could be personal data.

But it isn't as simple as that. An organisation may or may not use IP addresses in a way that is intended to identify or impact specific individuals. They may automatically be collected by its systems, but either not reviewed, or only used for gathering aggregated statistics on website visitors. Or an organisation may be unable to link the identity of someone making a SAR to the personal data associated with the IP address. So, if you receive a message from me asking for logs of my access to your website (which requires no credentials to access), can you be sure which IP addresses and therefore which logs relate to me?

BELOW An IP address is an online identifier and could be classed as personal data

Identifying the requestor

There is an interesting and often overlooked provision of the UK GDPR under Article 11: if the purposes for which personal data is processed do not require identification of an individual, the organisation need not maintain additional information in order to identify them. And, following on from this, if the organisation can demonstrate that it cannot identify them, the right of access (together with other rights of individuals) does not apply. But there's an exception. If the individual provides additional information to identify themselves, they will then have a right to access their data.

Even where Article 11 does not apply, where an organisation has reasonable doubts as to a requestor's identity, Article 12(6) allows it to ask them for additional information to confirm their identity (before addressing the request).

On an aside, where there is an issue with identification of someone making a SAR, I often hear a stock response of "we shall request a copy of the individual's passport and proof of address". Indeed, a passport contains several potential identifiers – full name, image, passport number and date of birth, while proof of address would mean you now know where the person lives. But how would that actually help you if your only dealings with them are online, and the records you hold don't include any of the same identifiers? What you have achieved is the collection of additional (possibly more sensitive) personal data leading to greater data protection risks in handling it. Identification checks need to be tailored to the context of your relationship with an individual.

Back to the query in hand – it was tricky! While the company did hold certain records by reference to an IP address, it couldn't at that stage be sure that the IP address uniquely identified the person making the request. It needed to consider, in relation to the records held, whether it was in a position to identify an individual, and whether the requestor could provide additional information to enable their identification.

Before moving on, we also need to keep an eye out for changes to the definition of "personal data" within the Data Protection and Digital Information Bill (which was introduced into Parliament in July 2022). The aim of these changes is to provide greater clarity on when an individual is identifiable.

Exemptions to right of access

Another organisation received a SAR from someone looking for information on decisions that had been made about them. Opinions and decisions about someone are that person's personal data, as the information "relates to" them. Information about reasons for a decision may also be personal data, to the extent it relates to the individual.

The organisation was concerned that releasing all records concerning relevant decisions would reveal confidential and proprietary information about its decision-making techniques. So the question to me was whether it could apply any exemptions.

The bulk of the exemptions can be found in schedules 2 to 4 of the UK Data Protection Act 2018 (which complements the UK GDPR). One that pops up a lot is "management forecasts". This applies where data is used for the purpose of management planning (for example, in relation to redundancies), and provision of that data would be likely to prejudice the conduct of the business. Which, for the query I received, was not the case.

Intellectual property

Let's take a look at an exception under Article 15(4) of the UK GDPR (relating to SARs): "The right to obtain a copy… shall not adversely affect the rights and freedoms of others." The data protection rights of other individuals most commonly spring to mind. But Recital 63 helps us to explore what else may be covered. It refers to the rights of others as including "trade secrets or intellectual property and in particular the copyright protecting the software" (the reference to what software being somewhat unclear).

The purpose of the right of access is transparency. Exemptions are there to protect other business or public interests, but should not be overused. It's also important that application of Article 15(4) requires a balancing test between the requesting individual's right of access and the intellectual property (or other rights) of the other party. Just because another right exists doesn't mean that Article 15(4) applies automatically – the importance of providing access to personal data can override the other right. In addition, perhaps curiously, it is an exception to the right to receive a copy of the data (under Article 15(3)), but not a general exemption to the right of access.

Taking all this into account, firms shouldn't take an all-or-nothing approach. They need to assess how much personal data they can still provide, and how to provide it, without unreasonably affecting other rights. A company could, for example, send reduced sets of data, or redact or extract data from records.

The reference to intellectual property rights in the UK GDPR is another frequently overlooked provision. Indeed, the ICO's guidance on exemptions doesn't seem to mention it at all. It is touched on, however, in the European Data Protection Board's guidelines on the equivalent right of access under the EU GDPR (Guidelines 1/2022). They give an example of a gamer being denied access to a gaming platform due to allegations of cheating, detected by anti-cheating software. The gamer makes a SAR and requests information about the reasons for the decision. The gaming platform should provide some information about the alleged cheating (such as dates and times, and what was detected), but may be able to withhold information concerning technical operating of the anti-cheat software if this is a trade secret (and, presumably, to protect copyright).

Another example in the Guidelines relates to a company's proprietary techniques for a medical assessment of an individual. If the person makes a SAR, the company may be able to withhold information about the results of the assessment to the extent this would reveal its techniques.

Back to the query I received. The organisation therefore needed to think about a few things: (a) what specific content concerning decisions was the requestor's personal data, and which decision-making techniques may be revealed by sharing this data; (b) whether its decision-making techniques gave rise to intellectual property rights (to be assessed under intellectual property laws); and (c) if so, how to balance those rights with the requestor's right of access. And then to reach a conclusion: what personal data could and should still be shared, and how?

ABOVE Individuals have the right to know how automated credit-scoring works

"The question to me was whether it could apply any exemptions"

BELOW Companies may not need to disclose techniques for conducting medical assessments

But since we're talking about decision-making, that's not all. As well as giving individuals a right to access personal data, Article 15(1) UK GDPR requires information to be provided about solely automated decision-making. This means decisions made by technological means without human involvement (such as, for example, automated credit-scoring). If these were taking place, the organisation must inform the requestor (among other matters) about the logic involved in those decisions. This does not necessarily mean sharing detailed algorithms, which may also prejudice intellectual property rights. But the information must be meaningful for the individual, to enable them to understand how the decision was made; for example, the key points considered in reaching the decision, and their relevance to and impact on the individual.

Final thoughts

There are challenges in handling subject access requests. Some may have a clear resolution (such as not retaining emails for 20 years, and asking your staff not to call your customers twerps). Others may be relatively untested issues where the legislation and guidance are not wholly clear. Where analysis of a tricky area is making your head spin (as often happens to me), it may be helpful to open up a dialogue with the requestor to try to find a solution together, such as how they may identify themselves. You should also keep clear records of your analysis and conclusions, including in relation to the application of exemptions, and how you have balanced your interests with transparency for the individual.

olivia.whitcroft@obep.uk