The breadth and complexities of health data

Victoria Hordern of Bates Wells discusses the conditions most likely to be relevant for the processing of health data, and any additional safeguards needed.

If I email you to ask you how you are, and you respond by email that you're not feeling well, am I processing your health data? At what point does information about a person become personal data concerning health? The GDPR states that personal data concerning health "should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject" (recital 35). Given how widely mental health conditions are now defined, that's a fairly broad concept. Moreover, the GDPR indicates that personal data concerning health includes information about a person's registration for health care services (e.g. doctor's appointments), any number or symbol that uniquely identifies an individual for health purposes, information from tests or medical examinations, as well as information on a disease, disability or disease risk, medical history and clinical treatment.

In February 2015, and under the previous Data Protection Directive 95/46/EC (Directive), the Article 29 Working Party (as it then was) (WP) responded to the European Commission following a request from the Commission for the WP to clarify the scope of the definition of data concerning health in relation to lifestyle and wellbeing apps[1]. In its response the WP confirmed its previous view that a "wide range of personal data…may fall into the category of health data" and it "represents one of the most complex areas of sensitive data"[2]. So information about smoking and drinking habits, data on allergies and membership of a patient support group are all data concerning health. The WP also stated that for data to qualify as health data "it is not always necessary to establish 'ill health'". Additionally because the concept of health data includes "disease risk" it can also include the potential future status of an individual that can be predicted due to their lifestyle, current medical status or hereditary factors. In effect, it is any data from which conclusions can be reasonably drawn about the health status of an individual. Most obviously in today's global crisis, information about someone's test results following a Covid-19 test is health data, as is information about their symptoms and information provided in a health questionnaire.

> Information about someone's test results following a Covid-19 test is health data, as is information about their symptoms.

Why is health data special category data?

Special category data under the GDPR is a sub-category of personal data and is a continuation of the concept of sensitive personal data under the Directive. The rules around the use of this type of data have always been strict – essentially it is prohibited unless an exception applies. The WP stated that the concept of sensitive personal data stems from the presumption that misuse of this data is likely to have more severe consequences for an individual's fundamental rights. In particular "misuse of health data, including drawing incorrect or unreliable conclusions, may be irreversible and have long-term consequences for the individual…"[3].

Significantly, under the UK Equality Act 2010 there are several protected characteristics that could be considered to be health data – disability, gender reassignment, and pregnancy and maternity. The Equality Act makes it unlawful to treat someone in a discriminatory way on the basis of a protected characteristic. In many cases, unlawful treatment would also involve processing data, which would then likely trigger the rules on the processing of health data. However, the Equality Act does not use the term "health". It uses "disability" so that the protected treatment is triggered where the individual is less able that a healthy person. In contrast under the GDPR, health data includes data both where a person's health is good and where a person's health is poor.

When can health data be collected?

As it is special category data under the GDPR, controllers need to have both a lawful basis under Article 6 (Lawfulness of processing) and rely on an exception under Article 9 (Processing of special categories of personal data). It's also important to ensure that the processing meets the requirement for fairness under Article 5 (1) (a). This states "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')."

The Article 6 discussions are usually fairly straightforward. If a controller knows that they will have to rely on explicit consent under Article 9, they will rely on consent under Article 6. But there are a few idiosyncrasies. While a controller can rely on a situation where collection of heath data is necessary for performance of a contract under Article 6, there is no equivalent provision under Article 9. Likewise, Article 6 permits processing where the controller is under a legal obligation to do so but Article 9 does not provide an equivalent provision. In many

instances, a controller will rely on the legitimate interest lawful basis under Article 6. However, that is not without its complexities. The legitimate interest basis requires a balancing test and it may not always be clear-cut that the interest of the controller overrides any prejudice to the individual's privacy rights.

Identifying an Article 9 exception for use of health data can be complicated. For a start, the GDPR permits Member States to introduce further conditions including limitations for processing health data[4]. So implementing a single approach that works across the EU can be difficult.

Employees: In the context of employee health data, reliance on consent is problematic given the requirement for consent to be freely given and the well-documented concern by data protection authorities that employees are unlikely to feel they can give free consent. In most instances, though, employers can rely on Article 9 (2)(b) for collecting health data on employees and arguably other types of workers including the self-employed. An employer can point to legal obligations it is subject to e.g. supporting sick employees or providing a safe place of work – taking the temperatures of employees before they enter the workplace is one example where an employer is complying with its health and safety obligations in today's world and employee consent is not required. The additional requirement under the UK Data Protection Act 2018 (DP Act) when relying on this exception is to put in place an appropriate policy document (APD) which is essentially an additional safeguard considered necessary by the UK Government[5].

Health: Two of the exceptions under Article 9 are more obviously geared towards the processing of health data – Article 9(2)(h) and (i). Provision (h) relates to purposes connected with medicine, medical diagnosis, provision of health care or treatment but there must be a professional bound by professional secrecy handling such data. Recital 53 states that where health data is processed for "health-related purposes" this should be "only where necessary to achieve those purposes for the benefit of natural persons and society as a whole". In other words, reliance on provision (h) should always involve a benefit.

Provision (i) relates to processing necessary for reasons of public interest in the area of public health and UK law stipulates that it must be carried out by a health professional or another person bound by a duty of confidentiality[6]. Recital 54 links the concept of "public health" to an EU Regulation concerned with statistics on public health and health and safety at work. Patently, concepts of benefiting society as a whole and protecting public health have strong resonances in today's global crisis.

What about a non-healthcare related controller wanting to collect health data on individuals who are not its employees or workers? If it's a non-profit it may be able to rely on Article 9(2)(d) but that exception is fairly narrow. Additionally if the health data has not been manifestly made public by the individual and is not connected with any legal claim the controller is facing or bringing, it's likely the only option will be explicit consent. Separately, Article 9(2)(j) will be relevant for organisations processing health data for archiving purposes or research purposes in the public interest.

Public interest: However, Article 9 allows Member States to set out their own grounds for reasons of substantial public interest and this is where Schedule 1 DP Act becomes relevant. The 23 substantial public interest conditions set out in Part 2 of Schedule 1 however don't lend themselves to easy interpretation. For a start, most have to be necessary for reasons of substantial public interest but there's no clear guidance what that means in practice. The conditions most likely to be relevant for the use of health data are (all paragraphs under Schedule 1):

- para 8: equality of opportunity or treatment;
- para 16: support by a non-profit for individuals with a particular disability or medical condition;
- para 17: counseling;
- para 18: safeguarding;
- para 19: safeguarding of economic well-being of individuals;
- para 20: for the insurance industry;
- para 21: occupational pensions.

Nevertheless, it is also possible that there are circumstances where a controller is collecting health data for the purposes of prevention or detection of an unlawful act (para 10) or protecting the public against dishonesty or other seriously improper conduct (para 11). In most instances, when using health data for a substantial public interest, controllers in the UK must put an Appropriate Policy Document (APD) in place.

> In the UK you are likely to have to complete an Appropriate Policy Document.

What further safeguards are required?

Health data is considered to be more intrusive into people's privacy and inevitably comes with greater protections. For instance, it may be necessary to carry out a Data Protection Impact Assessment (DPIA). This process is set out under Article 35 (and the Information Commissioner (ICO) provides guidance on its website). Though a controller might argue that it's not processing health data on a large scale, it is still prudent to carry out a DPIA (even if only light-touch) to document your understanding of the impact of your processing of health data on individuals and how you will take steps to safeguard any intrusive impact on individuals.

Additionally as referred to above, in the UK you are likely to have to complete an APD. Under Part 4 Schedule 1 DP Act, an APD must (for the use of the relevant special category data) explain the controller's procedures for complying with the data protection principles in Article 5 and specifically explain the policies regarding retention and erasure of this data setting out for how long the data is likely to be retained.

The ICO's guidance makes clear

that you only need one APD to cover all the processing that requires it. An APD should be drafted on the basis that it could be provided to affected individuals and to the ICO. Additionally, you must reflect this processing in your Record of Processing Activities document. The ICO's template APD sets out a series of questions which it expects controllers to answer and document their responses in the APD[7]. In many respects, the scope of what the template asks is what any well thought through data protection policy should cover within the controller i.e. addressing what the data protection principle is and what is required of the controller to meet that principle.

Operationally and technically, any use of health data should involve greater protections to prevent and deter misuse. Cybercriminals frequently target organisations that process health data whether public authorities or small companies. Organisations holding significant amounts of health data must be prepared to invest in resilient technical and operational security controls which are monitored, tested and kept up to date.

What are the implications in the current crisis?

Organisations are currently collecting more health data than normal whether that be on employees, customers or other service users. Countering the risk of the Covid-19 virus spreading is a priority for us all. Understandably for many businesses, they want to get back on track, and data protection compliance may not be a high priority. However, individuals still have privacy rights and the law has stipulated that any health data must be subject to stricter rules. Therefore, controllers must establish their lawful basis for collecting health data and document any DPIA and APD.

Of course, one of the questions looming is what happens with all the health data collected once the crisis has abated (or eventually is over)? Controllers need to be careful not to use the health data for unrelated purposes or to retain it beyond its use. They should be ensuring that they have a secure way of deleting health data once they no longer need it.

AUTHOR

Victoria Hordern is a Partner and Head of Data Privacy at Bates Wells.
Email: V.Hordern@bateswells.co.uk

REFERENCES

1 See: ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf, Letter to European Commission, DG CONNECT on mHealth, 5 February 2015.
2 *Ibid*, Annex, p 1.
3 *Ibid*, Annex, p. 1.
4 Article 9(4).
5 www.gov.uk/government/publications/hmrc-appropriate-policy-document#:~:text=The%20HMRC%20appropriate%20policy%20document,data%20and%20criminal%20convictions%20data.
6 DP Act, Schedule 1, para 3 (b).
7 privacylaws.com/media/3255/appropriate-policy-document-5.docx

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Binding Corporate Rules and Brexit – a practical way forward

Sian Rudgard of Hogan Lovells explains what the situation is for organisations that are considering applying for, or already have BCRs approved.

At the end of July, and so with only five months remaining until the end of the transition period, the European Data Protection Board (EDPB) issued an information note for companies that have the ICO as their lead authority as to the steps that they need to take in order to move their Binding Corporate Rules (BCR) application, or approved BCR, to an European

Continued on p.3

Gamify it! Making your data protection training stick

Using games to deliver DP training can be a fun and cost effective way to get your message through. By **Abigail Dubiniecki**, freelance data privacy lawyer and consultant.

Among the many DPO tasks, addressing the human factor is perhaps the most challenging. Effective training can transform an organisation's weakest link into its greatest asset. Yet compliance training is often met with eye rolls by staff, while senior managers see it as a necessary "one-and-done" evil. The result: managers chase employees, employees reluctantly comply, and DPOs continue to hand-hold or

Continued on p.5

New PL&B resources

- PL&B's Data Protection Clinic: Book a 30 minute consultation to help resolve your Data Protection issues. The clinic will support you in identifying your key priorities and much more.

www.privacylaws.com/clinic

- PL&B's *Privacy Paths* podcasts are available at www.privacylaws.com/podcasts and from podcast directories, including Apple, Alexa, Spotify, Sticher and Buzzsprout. Upcoming topics include the impact of the EU-US Privacy Shield's invalidation in the US

Issue 111 **SEPTEMBER 2020**

COMMENT

2 - Can the UK get EU adequacy?

NEWS

9 - Novel mechanisms for transfers?
18 - ICO replies on Covid-19 privacy

ANALYSIS

1 - BCRs and Brexit – a way forward
11 - Cloud v *Schrems 2*
14 - The complexities of health data

MANAGEMENT

1 - Making DP training stick
17 - Is it legal for employers to record video meetings?
19 - Cookie audit automation

FREEDOM OF INFORMATION

23 - ICO will not name underperformers

NEWS IN BRIEF

8 - Appeal partially in favour of DP rights in facial recognition case
10 - Test and Trace DPIA
10 - ICO children's code in force
13 - £100,000 fine for unsolicited marketing emails
13 - ICO statement on *Schrems II* case
16 - Marriott High Court class action
16 - ICO issues annual report
21 - Salesforce and Oracle class action
21 - Heathrow developing a facial recognition check-in function
21 - Lords call for Online Harms legislation this year
22 - Guernsey telco fined £80,000
22 - ICO say AI guidance will evolve
22 - Consultation on DP Act representative action provisions
23 - The ICO Innovation Hub continues

UNITED KINGDOM
report

ISSUE NO 111 **SEPTEMBER 2020**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS

Sian Rudgard
Hogan Lovells International LLP

Abigail Dubiniecki
Freelance data privacy lawyer

Edwin Baker, Alexander Dittel and Marta Dunphy-Moriel
Kemp Little LLP

Kathleen Morrison
Brodies LLP

Victoria Hordern
Bates Wells

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2047-1479

comment

Can the UK still get EU adequacy?

As the Brexit negotiations are in jeopardy due to the government's new Internal Market Bill, progress made on data protection and UK adequacy may also be hampered. If we end up with a no-deal, Standard Contractual Clauses (SCCs) will play a more significant role in international data transfers. But there are now new challenges caused by the *Schrems II* decision, also in relation to cloud computing (p.11).

The European Commission is currently working on a revised set of SCCs to take the judgment of the Court of Justice of the European Union into account. The European Commission says that this is a top priority for the coming months, with a view to finalising the clauses by the end of this year. Also, discussions have started with the United States to find a way forward. In the UK, the government's National Data Strategy seeks innovative mechanisms for international data transfers (p.9).

There is more certainty over the role of Binding Corporate Rules and changes to the ICO's remit after Brexit. Read our correspondent's analysis and practical advice on p.1.

The Appropriate Design Code is now in effect, and organisations have until 2 September 2021 to ensure compliance. The Code requires high privacy settings as a default. The ICO is issuing guidance and will host webinars on this topic (p.10). It is also keen to have submissions for its Sandbox programme on projects that deal with children's data.

For those who have responsibility for delivering data protection training, this issue brings a wealth of ideas on how to engage staff through data protection themed games (p.1). The aim is to make learning fun and encourage discussion on privacy issues.

The pandemic has changed the working life for many of us. DPOs are now often taking video calls and attending or organising online conferences and meetings. Which data protection rules do we have to keep in mind in this environment (p.17)? And which details are actually included in the broadly defined concept of health data (p.14)? The Information Commissioner responds to MPs' unease about privacy and Covid-19 (p.18) whilst seeing a massive impact on resources due to Covid-related work.

Last but not least, is cookie audit automation your get out of jail card? Find out on p.19 how technology can help the busy DPO.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access UK events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

"I've always found *PL&B* to be a great resource for updates on privacy law issues, particularly those with a pan-EU focus. It strikes the right balance for those in-house and in private practice. The content is clear, well presented and topical."

Matthew Holman, Principal, EMW Law LLP

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 33rd year. Comprehensive global news, currently on 165+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.