GIR Global Investigations Review

The Practitioner's Guide to Global Investigations

Volume I: Global Investigations in the United Kingdom and the United States

SIXTH EDITION

Editors
Judith Seddon, Eleanor Davison, Christopher J Morvillo,
Michael Bowes QC, Luke Tolaini, Ama A Adams, Tara McGrath

2021

The Practitioner's Guide to Global Investigations

Volume I: Global Investigations in the United Kingdom and the United States

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2021
For further information please contact insight@globalinvestigationsreview.com

40

Data Protection in Investigations

Stuart Alford QC, Serrin A Turner, Gail E Crawford, Hayley Pizzey, Mair Williams and Matthew Valenti[1]

40.1 Introduction

Data protection law is a misleading term, because the relevant framework will be a combination of employment, whistleblower, criminal and privacy laws. Companies and practitioners must navigate domestic and international legislation that touches on data protection, while ensuring they stay on the right side of regulatory and prosecuting agencies and co-operate with them to the extent that it is of benefit.

Handling data about individuals has become increasingly complex, particularly when the data protection regimes in different jurisdictions appear to impose conflicting obligations on data holders.

This chapter will look at both UK (including some European) and US laws and how they frame issues around investigations and data protection. We will look at internal investigations and those conducted by authorities, and provide some specific guidance in respect of data protection and whistleblowing regimes.

In the United Kingdom, a balance must be struck between compliance and regulatory obligations that require the processing of data as part of investigations, and the protection afforded to individuals caught up in those investigations, primarily under the UK General Data Protection Regulation[2] (UK

1 Stuart Alford QC, Serrin A Turner and Gail E Crawford are partners, and Hayley Pizzey, Mair Williams and Matthew Valenti are associates, at Latham & Watkins.

2 UK GDPR, available at https://www.legislation.gov.uk/eur/2016/679/contents; Keeling schedules for the UK GDPR and the DPA 2018, which show the changes made post-Brexit, are available at https://www.gov.uk/government/publications/data-protection-law-eu-exit.

GDPR), which effectively retains Regulation (EU) 2016/679 (EU GDPR)[3] in UK law following the end of the Brexit transition period, and the UK Data Protection Act 2018 (DPA 2018).[4] In September 2021, the UK government opened a public consultation on wide-ranging reform to UK data protection laws, including proposals for an expansive framework for international data transfers.[5] The consultation closed in November 2021; further policy and regulatory developments are expected as the proposed reforms take shape.

UK laws governing the interception and monitoring of communications may also require navigation in internal investigations. Although legislation protecting individuals' data has existed for years, the increased sanctions for breaches under the GDPR (maximum fines being the higher of £17.5 million/€20 million or up to 4 per cent of annual worldwide turnover), and increased regulatory focus on data privacy, mean that investigators must take the protections afforded to individuals more seriously than they did previously. Across Europe, the GDPR largely consolidated and harmonised the previous European data protection regime, but it does not necessarily simplify the issue between Member States. Each Member State may have its own laws in place as long as the basic standards of the GDPR are met; the GDPR is a floor and not a ceiling.

Furthermore, both the UK GDPR and the EU GDPR catch not only UK/EU corporations and global company groups with a UK/EU presence (including their use of personal data outside the UK/EU to the extent that use is intrinsically linked with their domestic activities), but also affect any corporations overseas and with no UK/EU presence that actively offer goods and services to, or monitor the behaviour of, individuals within the UK/EU, even if the data is stored overseas. Multinational organisations may be required to comply with both the EU GDPR and the UK GDPR, depending on the scope of the investigation in question.

In the United States, there is no uniform, omnibus federal privacy regime comparable to the GDPR. However, a patchwork of federal and state privacy laws may come into play in an internal investigation, particularly when reviewing and collecting employees' electronic communications. To minimise legal risk, companies should provide employees with clear notice that their electronic communications stored on company systems or devices are subject to monitoring and search.

Given the territorial reach of both the UK GDPR and the EU GDPR, US and multinational companies may have to grapple with both sets of compliance obligations in conducting an internal investigation or responding to criminal

3 Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN.

4 DPA 2018, available at https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

5 Data: A new direction (10 September 2021), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1016395/Data_Reform_Consultation_Document__Accessible_.pdf.

or regulatory investigations. Where a US or multinational company's obligations to comply with US legal demands for personal data conflict with GDPR limits on the processing and transfer of that data to the United States, the company must assess whether it can lawfully transfer responsive data to the United States that is subject to the UK GDPR or EU GDPR, or both. This assessment is all the more important, and complex, in light of the Court of Justice of the European Union's (CJEU) decision in *Schrems II* (applicable in the United Kingdom and the European Union).[6] That decision invalidated the EU-US Privacy Shield (the framework designed to regulate the exchange of personal data from organisations in the EU to Privacy Shield-certified organisations in the United States), and imposed a number of caveats on the use of the standard contractual clauses (SCCs) (an alternative to the EU–US Privacy Shield as a data transfer mechanism) to transfer personal data to the United States. If the US or multinational company cannot lawfully transfer responsive data to the United States, it may need to negotiate with the requesting legal authority to narrow the scope of the request or to develop other ways of resolving the legal conflict. Where the conflict cannot be resolved, the US or multinational company may need to consider challenging the request on comity grounds, although such challenges have rarely succeeded in criminal or regulatory investigations.[7]

40.2 Internal investigations: UK perspective

Internal investigations will inevitably deal with personal data, particularly employees' data, which in the United Kingdom is governed by the UK GDPR and DPA 2018. For those conducting internal investigations, the key obligations to consider are:

- transparency, namely the requirement to inform individuals about how their personal data is being used (unless there is a relevant exemption);
- data minimisation, namely the requirement to ensure that use of personal data for the investigation is proportionate;
- establishing a legal basis for the processing of personal data, as prescribed by the UK GDPR (consent and legitimate interest are two of the legal bases companies and practitioners can commonly rely on to process data in an internal investigation);

6 *Data Protection Commissioner v. Facebook Ireland Limited, Maximilian Schrems* (Case C-311/1).

7 See *In re Grand Jury Subpoena dated Aug. 9, 2000*, 218 F. Supp. 2d 544, 554 (S.D.N.Y. 2002) ('Courts consistently hold that the United States interest in law enforcement outweighs the interests of the foreign states in bank secrecy and the hardships imposed on the entity subject to compliance.') (collecting cases); see also *In re Grand Jury Proceedings*, 532 F.2d 404 (5th Cir.), cert. denied, 429 U.S. 940 (upholding grand jury subpoena against comity challenge based on foreign banking privacy laws).

- if applicable, establishing a relevant condition on which to process any 'special categories' of personal data or any criminal offences data involved (in addition to a legal basis for the processing), and;
- if personal data will be transferred, or accessed from, outside the United Kingdom, ensuring a legal basis for that data transfer, as prescribed by the UK GDPR (in addition to a legal basis for the underlying processing).

Transparency 40.2.1

The UK GDPR and DPA 2018 require relevant organisations to inform individuals in advance about how their personal data is processed, in a clear and accessible manner, and prescribe the minimum information to be provided.[8] Meeting these obligations in internal investigations can present practical challenges if an organisation does not have a comprehensive monitoring policy, as use of employees' personal data for investigation purposes may well be detrimental to, and unexpected by, those employees.

There are certain exemptions under the DPA 2018 to the specific obligation to provide minimum information to individuals. When collecting personal data directly from an individual, organisations need not provide data protection information that the individual already has. This may be relevant for organisations conducting investigations into, or involving, their employees and using personal data the organisation has obtained from them, if the organisation already provides some level of privacy information to them. A wider range of exemptions are available in circumstances where the personal data is obtained from other sources. The most relevant exemptions in internal investigations apply if providing the information to the individual would be impossible or would involve disproportionate effort, or would render impossible or seriously impair achievement of the objectives of the processing; or the organisation is required by law to obtain or disclose the personal data (under a binding legal obligation, rather than, for example, compliance with a non-binding code of practice, an informal, non-binding regulator request or a contractual obligation).

In addition to the transparency principles under the UK GDPR, the United Kingdom's regulatory framework for communications monitoring also requires organisations to be transparent with employees about the interception and monitoring of their communications (in written policies and in consistent business practices). Taken together, in internal investigations, the data protection and communications regimes oblige organisations to be clear and open with employees about how their personal data and communications are used, and to ensure that any interception and subsequent review, use and disclosure of data and communications in an investigation is lawful and proportionate. Robust, clear and accessible data privacy information notices for employees,

8 This minimum information includes, among other things, the purposes of the processing, the lawful basis for the processing, the recipients or categories of recipients of the personal data, details of data transfers outside the United Kingdom and applicable data retention periods.

and policies on employee monitoring, will provide a valuable shield against claims of employee privacy infringement and non-compliant monitoring practices – at least in the United Kingdom.[9]

40.2.2 Data minimisation

The UK GDPR principle of data minimisation should be applied by organisations across their personal data activities generally, including internal (and external) investigations. Organisations should ensure that the collation, review, use and disclosure of individuals' data during the investigation is proportionate and no more intrusive than is necessary to achieve the legitimate purposes of the investigation. This will be relatively straightforward for clearly defined and focused investigations, but may prove more challenging to assess in practice in wide-ranging investigations requiring significant levels of data for loosely defined purposes. Organisations would be well advised to document the investigation's scope and associated personal data proportionality assessment, to demonstrate that data minimisation principles have been applied. Practical safeguards to ensure proportionality should also be applied, such as appropriately limiting the scope of documentation, email and communications review and disclosure (limiting impacted custodians and individuals, using keyword searches and time periods to identify relevant information, etc.).

40.2.3 Legal basis for data processing: consent

Consent from individuals provides a legal basis for the processing of their personal data, provided the UK GDPR consent conditions are met. Consent must be given freely and clearly, and in plain language, and must be an affirmative act – consent cannot be given by inactivity, such as pre-ticked boxes in an online form.[10]

In the typical employer–employee context of an internal investigation, the concept of consent being freely given is complicated. Given the dynamic, some jurisdictions consider that consent from an employee to an employer may never be freely given,[11] a position exacerbated in an internal investigation by the added element of potential wrongdoing by the employee or another individual, and tipping-off considerations. Investigators should ensure they comply

9 The position in a number of European jurisdictions (including France and Germany) is considerably more protective of employee rights and restrictive of an employer's ability to intercept or review communications or to access employee devices.

10 UK GDPR, Article 7 and Recital 32.

11 The European Data Protection Board's (EDPB) Guidelines on consent under the EU GDPR deem reliance on consent to be 'problematic' in an employment context, and recommends that it is not relied on other than in exceptional circumstances. Guidelines 05/2020 on consent under Regulation 2016/679 (4 May 2020), at p. 9, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf. The UK Information Commissioner's Office (ICO) considers that the EDPB's guidelines and opinions may offer guidance in applying the UK GDPR, in the absence of UK-specific guidance or regulations.

with the UK GDPR, either by getting express consent from the data subject to process their data, which may not be feasible in an internal investigation if it cannot be considered freely given or because the organisation does not want to notify the individual of the investigation (blanket clauses in employment contracts will no longer be enough), or by relying on another lawful basis under the UK GDPR to lawfully process the data.

Legal basis for data processing: legitimate interest 40.2.4

The UK GDPR provides a number of other legal bases for the processing of personal data in certain circumstances.[12]

Under the UK GDPR, an organisation can consider the legitimate interests of a third party or public interest, as well as its own legitimate interests, when assessing the use and processing of personal data.

In an internal investigation, this ability could allow an organisation to rely on the lawful basis of legitimate interests (of a third party or public interest) to process personal data. The rights of individuals can, however, override a legitimate interest, if the effect on an individual's interests or fundamental rights override the organisation's (or a third party's) legitimate interests.

The Information Commissioner's Office (ICO) enforces data protection legislation and has stated: 'Legitimate interests is the most flexible lawful basis for processing.' The ICO has set out a three-part, cumulative test for establishing whether there is a legitimate interest in processing the data, which may be a useful addition to an investigation plan:

- Purpose test: is the purpose of the processing a legitimate interest?
- Necessity test: is the processing of the data necessary and proportionate for the purpose?
- Balancing test: is the legitimate interest overridden by the individual's interests, rights and freedoms?[13]

The above test can be used by those conducting internal investigations to justify the processing of data under the UK GDPR because it is for the legitimate purpose of the company itself, or a third party, provided any risk of undue harm to the individual does not outweigh that interest.[14] In respect of the necessity test, companies must consider whether there is an alternative, less intrusive, means of gathering or processing the same information.

12 UK GDPR, Article 6.

13 'Legitimate interests' (ICO), available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.

14 The UK government's proposed data protection reforms include a proposal to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test. The proposed list includes the following interests that may be relevant in investigations: the reporting of criminal acts to appropriate authorities; and improving or reviewing an organisation's system or network security. The government is seeking views on both the creation of a list and on the interests and activities to be included.

To demonstrate compliance with the UK GDPR, organisations will have to document their decisions carefully (through a legitimate interests assessment).[15]

40.2.5 Special category and criminal offences data

When processing data in an internal investigation, data controllers must pay increased attention when dealing with special category data.[16] In an internal investigation, this kind of information will often be held in a human-resources file that becomes part of a review within the investigation. Employee emails or instant messages, etc., could possibly be considered special category data, as they could potentially contain data within this definition. However, it is certainly arguable that emails should not fall into this category on the basis that any special category data is incidental and not part of the primary purpose of the use of data in that context. This argument is strengthened by the application of data minimisation steps to ensure the special category data is not specifically identified or targeted as part of the investigation.

When dealing with special category data, organisations must establish both a legal basis for the data processing (e.g., consent, legitimate interests or another basis under the UK GDPR) and an additional, specific legal basis for processing the relevant special category data. The UK GDPR and DPA 2018 provide for a number of specific legal bases or conditions for the use of special category data.[17]

Information about criminal allegations, proceedings or convictions in relation to an individual may also be relevant in an internal investigation. This data is treated separately to special category data under the UK GDPR, and requires a lawful basis for processing and legal or official authority to handle that data, which must be prescribed under national law. In the United Kingdom, the UK GDPR and DPA 2018 authorise the processing of criminal offences data in limited circumstances and subject to the conditions set out in the UK GDPR and DPA 2018.[18] These legal authority grounds are narrow, though some may be available in internal investigations, including prescribed public interest grounds, consent of the individual and establishing or defending a legal claim. Special category data and criminal convictions data should be handled with particular consideration, and organisations should ensure that the basis on which they are using this data is clearly documented.

15 ibid.

16 Special category data is defined in the UK GDPR and the DPA 2018 as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation' (UK GDPR, Article 9; DPA 2018, s.10).

17 UK GDPR, Article 9; DPA 2018, ss.10 and 11 and Schedule 1.

18 UK GDPR, Article 10; DPA 2018, ss.10 and 11 and Schedule 1.

Public interest 40.2.6

The public interest ground for processing special category or criminal offences data may be useful in an internal investigation, especially where it is likely to be followed by a regulatory investigation, and where consent or another legal basis is not available in practice. This ground is limited to those public interest purposes that are specifically provided for in national law. Under the DPA 2018, these public interest purposes are relatively narrowly defined, meaning this ground will be difficult to satisfy in practice, and organisations should be confident in, and have clearly documented, their justifications before relying on this basis.

Under the DPA 2018, the public interest purposes of particular relevance to internal investigations relate to the prevention or detection of unlawful acts, and to protecting the public against dishonesty, in both cases provided there is also a 'substantial public interest'.[19] Both provisions require that processing be done without consent of the individual, to avoid prejudicing the investigation. As the scope of the public interest ground for data processing (under the EU GDPR as well as the UK GDPR) must be provided for under national law, it may vary across the European Union. Organisations should therefore seek local legal advice in the relevant Member States.

Data transfer outside United Kingdom and European Economic Area 40.2.7

Given the international scope of many investigations, companies should consider the practicalities of exporting data while complying with the UK GDPR and the EU GDPR (as applicable). If the personal data will be transferred, or accessed from, outside the UK or European Economic Area (EEA) – whether from within the organisation's corporate group or externally – that data transfer also requires a separate lawful basis under the UK GDPR or EU GDPR, in addition to the lawful processing of the data itself. This restriction on data transfers does not apply to third countries recognised as 'adequate' by the UK Secretary of State or the European Commission respectively, to which personal data may be transferred freely.[20] Following Brexit, relevant adequacy decisions have been passed by the European and UK authorities to permit the unrestricted transfer of personal data between the EEA and the United Kingdom.

On 16 July 2020, in the *Schrems II* decision, the CJEU invalidated the European Commission's EU–US Privacy Shield Adequacy Decision

19 DPA 2018, Schedule 1, Part 2.

20 For transfers under the EU GDPR, the European Commission has recognised the following countries as having adequate protection: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, United Kingdom and Uruguay. An adequacy decision in relation to South Korea is being adopted. For transfers under the UK GDPR, the UK Secretary of State has recognised the following countries as having adequate protection: all EEA jurisdictions, Gibraltar and jurisdictions recognised as adequate by the European Commission, as at 31 December 2021.

(2016/1250), one of the key mechanisms for lawfully transferring personal data from the EEA to Privacy Shield-certified organisations in the United States, on the basis that the Privacy Shield did not provide an 'adequate' level of protection required under the GDPR for the transfer of data from the EEA to the United States.[21] In the same judgment, the CJEU ruled that SCCs[22] remain valid in respect of any personal data export (not just EEA–US transfers), but imposed caveats on their use.

The data transfer safeguard most commonly relied on in investigations, for intra-group transfers within an organisation or to or from third-party providers involved in the investigation, consists of using SCCs. These are European Commission approved standard-form contractual agreements that put in place binding data protection obligations between the data exporting and importing entities. On 4 June 2021, the European Commission issued revised SCCs for data transfers subject to the EU GDPR,[23] which replace the previous SCCs from 27 September 2021 (though contracts under the previous SCCs in place on this date may be relied on until 27 December 2022, by when all previous SCCs must be migrated to the revised SCCs). The revised SCCs are not recognised for data transfers subject to the UK GDPR, for which organisations should continue to rely on the previous SCCs, until the ICO's revised data transfer mechanisms under the UK GDPR are in effect.[24]

Following the *Schrems II* decision, organisations seeking to rely on the SCCs, for data transfers subject to the UK GDPR or the EU GDPR and pursuant to the revised or the previous SCCs, must assess, case by case, whether the law of the destination country ensures adequate protection for the personal data being transferred, and to put in place supplementary measures to ensure an essentially equivalent level of protection if required.[25] In relation to data transfers to the United States specifically, the CJEU found that, in its judgment and in the context of the Privacy Shield, the US legal regime does not ensure

21 *Data Protection Commissioner v. Facebook Ireland Limited, Maximilian Schrems* (Case C-311/1).

22 Sometimes referred to as the 'Model Clauses'.

23 Available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en.

24 On 11 August 2021, the ICO opened a consultation on its proposed, revised data transfer package under the UK GDPR, which includes an International Data Transfer Agreement to replace the previous SCCs, and a UK Addendum to the revised SCCs intended to allow the revised SCCs to be used for data transfers under the UK GDPR.

25 The EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (available at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en) set out the EDPB's recommendations and guidance on how the required assessment may be carried out and provides of examples of potential supplementary measures. The ICO's proposed data transfer package includes an international transfer risk assessment and tool, which provides guidance and a framework for conducting the required assessment for UK GDPR transfers.

an essentially equivalent level of protection. The CJEU was particularly focused on access rights to data by US public authorities for national security purposes, and associated individual rights and remedies. In light of the evolving SCCs requirements and enforcement landscape in practice, organisations should carefully consider use of the SCCs to validate data transfers to the United States in internal investigations, whether under the EU GDPR or the UK GDPR, and document any data transfer assessments and any supplementary measures.

There are alternatives to the SCCs, though they may not be as reliable in practice for organisations conducting investigations. This includes the explicit consent of the individuals, and transfers required to establish or defend a legal claim (applicable for occasional transfers only).

Different data transfer considerations apply in investigations by authorities.

Third parties to investigations 40.2.8

Companies and practitioners often rely on third parties to assist with internal investigations (for example, in data analysis, legal advice or document review). These third parties will often need access to personal data. The UK GDPR requires that a contract (or equivalent legal act) is put in place where controllers engage the services of processors.

This contract must set out, among other information, the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller, as well as prescribed contractual obligations, including an obligation of confidentiality.[26]

Monitoring employees' electronic communications 40.2.9

A framework of regulations is in place in the United Kingdom to govern the extent to which employers can intercept and monitor their employees' electronic communications.[27] These communications regulations are triggered upon 'interception' of communications, defined as making the content of the communication available to a person who is not the sender or intended recipient, whether before, during or after transmission of the communication. In internal investigations, this will most likely be relevant when considering investigation-specific interception and monitoring of employee communications, or when assessing the legality of an organisation's communications monitoring practices.

The default position is that employers may not intercept employee communications other than with the consent of both the sender and the recipient of

26 UK GDPR, Article 28(3).

27 This framework consists primarily of the Investigatory Powers Act 2016 (IPA 2016); the Interception of Communications Code of Practice under the IPA 2016; and the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 (Business Interception Regulations) enacted under the IPA 2016.

the communication, or as authorised by the exemptions built into the legal framework. In practice, organisations carrying out internal investigations are most likely to rely on exemptions that permit interception: to monitor employee or external users' compliance with rules governing use of the system (whether internal policies or legal or regulatory requirements); to maintain records and establish facts; to prevent or detect crime; or for information security purposes.[28] If consent is relied on for interception purposes, this should be distinguishable from any consent relied on for UK GDPR purposes (which sets a higher consent standard), so that both interception and data protection consents can be evidenced if required.

40.3 Internal investigations: US perspective

The United States has no single unified data protection regime. However, a patchwork of federal and state privacy laws impose various constraints on the extent to which a company may collect and review information about its employees, particularly their electronic communications.

State privacy laws in the United States vary considerably, but many states recognise a common-law right against unreasonable intrusions into a person's seclusion or privacy. Such causes of action have arisen against employers following searches in the workplace.[29] Accordingly, companies are well advised to have written policies, that all employees must acknowledge, clearly providing that the company's network and systems are subject to monitoring and search.

Other state laws place more specific prohibitions on employers that can limit the outer bounds of a company's investigative actions, for example prohibiting questioning an employee on issues that serve no business purpose,[30] or demanding an employee disclose passwords and other credentials to personal email and social networking accounts.[31]

Various state and federal laws also restrict the collection of electronic communications, including emails (work and personal), phone calls[32] and social

28 Provided for under the Business Interception Regulations and the Interception of Communications Code of Practice.

29 See, e.g., *Rowe v. Guardian Auto. Prods*., 2005 WL 3299766 (N.D. Ohio 6 December 2005); Restatement (Third) of Emp't Law: Emp't Privacy & Autonomy ch. 7 (Council Draft No. 6, 2011), available at http://extranet.ali.org/docs/Employment_Law_CD6_online.pdf (introducing the tort of wrongful employer intrusion upon a protected employee privacy interest and stating that '[e]mployees have a right of privacy against wrongful employer intrusions upon protected employee privacy interests' including personal information').

30 See 2 Cal. Code Regs. § 7286.7(b) (prohibits employers from inquiring into any issues that otherwise serve no 'business purpose').

31 See, e.g., Cal. Labor Code § 980.

32 Some states require the consent of all parties to legally record a phone call. See, e.g., Cal. Penal Code § 630 et seq. (2006); Conn. Gen. Stat. § 52-570d (2006); Fla. Stat. §§ 934.01 to .03 (2005); 720 Ill. Comp. Stat. 5/14-1, -2 (2006); Md. Code Ann. Cts. & Jud. Proc. § 10-402 (2006); Mass. Gen. Laws ch. 272, § 99 (2006); Mont. Code Ann. 45-8-213; N.H. Rev Stat. Ann. §§ 570-A:l,

media accounts.[33] One primary federal law is the Electronic Communications Privacy Act,[34] which breaks down into the Wiretap Act (regulating interception of electronic communications),[35] the Pen Register Statute (regulating use of a pen register to track communications)[36] and the Stored Communications Act (regulating unauthorised access to stored electronic communications).[37] These statutes do not generally prohibit an employer from searching its own email system.[38] However, they may limit an employer's ability to use company-owned equipment to access an employee's communications stored with third-party providers (e.g., Gmail),[39] at least without the employee's consent. Other state laws govern an employer's ability to collect and use biometric data like fingerprints, voice prints or vein patterns from employees. One such law is the Illinois Biometric Information Privacy Act, which requires informed written consent prior to collection of biometric information.[40]

Finally, besides state and federal laws, internal investigations in the United States may also be subject to extraterritorial GDPR restrictions. In particular,

---

570-A:2 (2005), as amended by New Hampshire Laws Ch. 169 (H.B. 1353) (2016); 18 Pa. Cons. Stat. § 5701 et seq. (2005); Wash. Rev. Code § 9.73.030 (2006). Other states require just one party consent. See, e.g., Ariz. Rev. Stat. Ann. § 13-3005; D.C. Code Ann. § 23-542(b)(3); N.Y. Penal Law § 250.00(1); N.J. Rev. Stat. § 2A:156A-4(d); Ohio Rev. Code Ann. § 2933.52(B)(4); Tex. Penal Code Ann. § 16.D2(c)(4).

33 See, e.g., Cal. Lab. Code § 980; 19 Del. Code § 709A(b); Md. Code Lab. & Empl. § 3-712(b)(1); Nev. Rev. Stat. § 613.135; N.H. Rev. Stat. § 275:74; 820 Ill. Comp. Stat. § 55/10(b)(1).

34 See 18 U.S.C. §§ 2510-22, 2701-12.

35 Id., at §§ 2511–2522.

36 Id., at §§ 3121–3127.

37 Id., at §§ 2701–2711.

38 Id., at § 2701; see, e.g., *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d Cir. 2003) (holding that the insurance company that leased a computer system to an agent did not violate the Electronic Communications Privacy Act (ECPA) when it retrieved stored emails from computers); see also *Scott v. Beth Israel Med. Ctr., Inc.,* 17 Misc. 3d 934 (Sup. Ct. N.Y. Cty. 2007) (holding that a policy that employees had no privacy right over material created, received, saved, or sent using the employer's computer system sufficient to eliminate any expectation of privacy); *United States v. Etkin*, 2008 U.S. Dist. LEXIS 12834, at *14 to 16 (S.D.N.Y. 20 February 2008) (employees do not have a reasonable expectation of privacy when employers warn the employees via log-on notices or flash-screen warnings of a policy through which the employer could monitor or inspect the computers at any time); *United States v. Angevine*, 281 F.3d 1130, 1135 (10th Cir. 2002) (holding no reasonable expectation of privacy where an employer's policy 'clearly warned computer users [that] data [wa]s "fairly easy to access by third parties"'); *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) (holding that any reasonable expectation of privacy employee had in his work computer was eliminated when the employer announced that it could inspect the computer).

39 See 18 U.S.C. § 2701(a); see, e.g., *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 757, 758 (N.D. Ohio 2013) (denying an employer's motion to dismiss claims under the ECPA where an employee alleged that her supervisor accessed unopened emails from her Gmail account through her employer-issued BlackBerry).

40 740 ILCS 14/1 (2008); id., at § 10.

to the extent the investigation requires review of personal data stored in the United Kingdom or European Union – for example, an employment file for an employee in a UK or EU affiliate, stored locally – then the company must evaluate whether (1) the affiliate has a legal basis on which to disclose the data to the United States, (2) transparency obligations have been met and relevant information or notices have been provided (or an exemption applies), (3) data minimisation and proportionality principles have been applied and (4) one of the conditions for the transfer of personal data to the United States has been met. If the organisation cannot meet the requirement to legitimise the transfer, the company may wish to consider ways of handling the data that do not involve transferring personal data to the United States – such as reviewing the relevant personal data in the United Kingdom or European Union, or redacting personal information from the data set before it is transferred.

40.4 Investigations by authorities: UK perspective

Companies have always had to consider competing interests when dealing with investigating authorities, but, data protection has, historically, rarely been near the top of any list of considerations. The very significant fines available under the UK GDPR mean that companies must take data protection much more seriously, particularly the disclosing of personal data to authorities in the United Kingdom and overseas. The ICO has shown that it will not hesitate to use its powers under the UK GDPR to investigate and issue significant fines for breaches. In October 2020, the ICO fined British Airways £20 million for failing to protect the personal and financial details of more than 400,000 of its customers impacted by a data breach.[41] Later the same month, the ICO fined Marriott International Inc £18.4 million for infringements of the GDPR stemming from a data breach at Starwood, which Marriott acquired in 2016, affecting millions of individuals.[42] Although these represent a reduction of nearly 90 per cent and 81 per cent, respectively, from the originally proposed fines, the British Airways fine represents the largest fine imposed by the ICO to date for breach of the GDPR. It remains to be seen whether this initially robust approach to UK GDPR enforcement from the ICO will extend into the more nuanced environment of internal and regulatory investigations, with their frequently competing legal obligations. Moreover, following Brexit, organisations managing investigations that span the United Kingdom and European Union may be subject to, and exposed to enforcement under, both the UK GDPR and the EU GDPR.

41 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/.

42 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data- secure/.

Providing data to authorities 40.4.1

Where authorities make requests for data, companies must be absolutely clear about the legal powers by which those requests are being made, to ensure that they can comply with the request while fulfilling their UK GDPR obligations. The benefits of voluntarily handing over more data than specifically required have probably disappeared with the UK GDPR's tougher data regulation regime. Among other things, the UK GDPR requires organisations to be transparent and provide information to individuals, to minimise use of personal data, to establish a legal basis for processing personal data and to legitimise any transfers of data outside the United Kingdom (and the EEA, under the GDPR). These obligations apply equally in data disclosures to authorities.

In relation to establishing a relevant legal basis for data processing, as well as the grounds discussed above (consent, legitimate interests, etc.), the 'legal obligation' basis may be relevant in responding to information requests and investigations by authorities. The UK GDPR and DPA 2018 provide that personal data may be disclosed to comply with a legal obligation (excluding contractual obligations), but only to the extent necessary to comply with that legal obligation: a proportionality test applies. This ground can only be relied on to justify data processing where a clear and binding legal obligation is present, under UK law. Obligations originating from outside the United Kingdom provide no legal basis for data processing on this ground, even where those obligations may be binding on a non-UK entity within an organisation's global corporate group, for example. Organisations should carefully document the relevant legal obligation, and the associated assessment of necessity and proportionality, to evidence UK GDPR compliance.

In international investigations, companies will need to address the GDPR restrictions and requirements for the transfer of personal data outside the United Kingdom or EEA. The considerations for organisations disclosing data to third-party authorities are slightly different from those concerning internal investigations. For example, reliance on individual consent or the SCCs is unlikely to be practicable. Transfers necessary to establish or defend a legal claim may be a helpful relevant ground in this context, though it is only available for occasional transfers, so may not be appropriate in ongoing investigations or longer-term engagement with authorities. An alternative basis to consider is provided by the EU GDPR and UK GDPR regime requirements for transferring data under international agreements, such as mutual legal assistance treaties (MLATs).[43] Using MLATs provides a structured system for exchanging information and evidence, but the process can be expensive and lengthy, which is particularly unhelpful where credit for early and responsive co-operation is sought, particularly when dealing with US authorities. The 2019 UK–US Bilateral Data Access Agreement aims to alleviate these

43 EU GDPR, Article 48; the UK GDPR does not mirror this specific provision, but the United Kingdom does recognise certain treaties on mutual legal assistance.

concerns by providing a streamlined alternative to the MLAT process, though it is limited in scope to certain communications data held by communications services providers.[44]

As a general position, companies should be cautious when transferring data, even in response to requests from authorities.

Some national regulators (such as the Financial Conduct Authority and the US Securities and Exchange Commission) have reciprocal arrangements in place to transfer data. The use of these inter-regulator arrangements has a number of attractions. However, they often operate through a memorandum of understanding between the regulators, which on its face does not satisfy the definition of a legal agreement under Article 48 of the UK GDPR and so may not be an appropriate method for data transfer. While the interpretation of Article 48 of the UK GDPR remains untested, caution should be taken about permitting data to be transferred outside the jurisdiction under a memorandum of understanding between regulators.

See Chapters 11 and 12 on production of information to authorities

An alternative method for complying with the UK GDPR may be to redact personal information before handing documents over to authorities, depending on the size of the document set. This may, however, be a very expensive way of satisfying the authorities and the UK GDPR, particularly as it would require not only the data subject's name to be redacted, but also any information from which the data subject could be identified. Further, determining the appropriate approach to redaction is not always straightforward: data should be sufficiently redacted to satisfy the UK GDPR, but undue redaction may not be welcomed by the receiving authorities.

40.5 Investigations by authorities: US perspective

As in the United Kingdom, companies in the United States must be mindful of GDPR restrictions in responding to subpoenas or other compulsory demands requiring the production of documents. Under US law, a company served with compulsory demands must produce any responsive documents within its possession, custody or control – wherever the data is stored. To the extent that responsive data is stored in the European Union, and contains personal data subject to the UK GDPR or EU GDPR, the company must produce it notwithstanding its foreign location. As a result, US companies served with formal demands to produce documents may face a situation where their obligations to comply with US legal process conflict with the GDPR restrictions.

44 The UK–US Bilateral Data Access Agreement (signed on 3 October 2019) allows both US and UK law enforcement authorities to ask respective domestic courts to issue electronic data production orders directly against communications services provides in the other country, without going through the MLAT process. The text can be found at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

A US company concerned that it faces a conflict should first discuss the issue with the regulator or law enforcement agency involved and attempt to narrow the scope of the request to avoid or minimise the need to produce data regulated under UK GDPR or EU GDPR. This is particularly important because, for the company to rely on the legal defence derogation to produce the data to US authorities, the data must be '*necessary* for the establishment, exercise or defence of legal claims'.[45]

At the same time, US law enforcement authorities or regulatory agencies are likely to put the burden on the US company to show that the GDPR prevents the transfer and requires the company to identify all available bases to produce the documents.[46] Although the risk of breaching GDPR obligations should be a major consideration when dealing with investigating authorities, companies must balance this against the risks of non-compliance with US authorities, which may seek sanctions (including even criminal contempt) against a company for failing to comply with investigators' demands.

Where a company truly cannot comply with a demand for documents from US authorities without violating the transfer restrictions, and the company is unable to negotiate an adequate resolution with the US authorities, the company may choose to challenge the legal process. US courts have long held that, where it would violate foreign law for a company to produce certain documents in response to US legal process, the company may challenge enforcement based on international comity.

However, while courts have sometimes quashed subpoenas on comity grounds in civil litigation,[47] they have typically rebuffed such challenges of criminal investigations, finding that the domestic interest in enforcing the criminal laws trumped the foreign data privacy interests.[48] On the other hand, the prospect of significant GDPR penalties may lead US courts to give more weight to foreign data privacy interests than they might otherwise. Indeed, US court decisions applying the international comity balancing test have

45 UK GDPR, Article 49 / EU GDPR, Article 49 (emphasis added).

46 https://www.justice.gov/archives/opa/blog-entry/file/838386/download (US Department of Justice asserting that '[w]here a company claims that disclosure is prohibited, the burden is on the company to establish the prohibition. Moreover, a company should work diligently to identify all available legal bases to provide such documents').

47 See, e.g., *In re Cathode Ray Tube (CRT) Antitrust Litig.*, 2014 WL 1247770 (N.D. Cal. Mar. 26, 2014); *Motorola Credit Corp. v. Uzan*, 293 F.R.D. 595 (S.D.N.Y. 2013); *Tiffany (NJ) LLC v. Forbse*, 2012 WL 1918866 (S.D.N.Y. 23 May 2012).

48 See, e.g., *United States v. Davis*, 767 F.2d 1025, 1033-34 (2d Cir. 1985) (according deference to judgment of Executive Branch that interest in enforcing criminal laws outweighed interest of Cayman Islands in preserving privacy of its banking customers); *In re Grand Jury Proceedings*, 532 F.2d 404 (5th Cir.), cert. denied, 429 U.S. 940 (upholding a grand jury subpoena against comity challenge based on foreign banking privacy laws).

sometimes turned, in significant part, on the low likelihood of severe penalties being imposed by foreign authorities.[49]

40.6 Whistleblowers

The interplay between the increased protections for individuals under the UK GDPR and the protections for whistleblowers under existing laws is particularly interesting for practitioners and companies. More and more, internal and government investigations are triggered by information from (often anonymous) whistleblowers. Senior managers must be acutely aware of the respect to be shown to whistleblowers and whistleblowing laws, in particular with regard to anonymity and protection of the individual. The protection for whistleblowers is set to be strengthened across Europe, with the requirement on national legislatures to implement the EU Directive on whistleblowing protections by 17 December 2021.

40.6.1 Whistleblowing policies and data protection

Companies should have in place whistleblowing policies that respect the data protection principles – including specific whistleblower anonymity and privacy protections applicable in some jurisdictions – while also providing safeguards for the subject of the whistleblowing report, the whistleblower and third parties mentioned in the report. Companies must also ensure that by default, only personal data necessary for the specific purpose of investigating a whistleblowing report is processed.

40.6.2 Right to access

Where an individual's personal data has been processed during an investigation following a whistleblower report, the individual will still have the rights to access certain information as they would have done in any other circumstances. This includes the purpose and period envisaged for processing and how the data will be stored.[50] The personal information in a whistleblowing report can relate to whistleblowers, the persons under investigation, witnesses or other individuals mentioned, meaning that companies will need to uphold the data protection rights of all involved.[51]

---

49 Compare, e.g., *First City Nat'l City Bank*, 396 F.2d at 905 (compelling production of records notwithstanding potential conflict with German law, based in part on finding that the 'risk of civil damages [being imposed under German law] was slight and speculative') with, *Tiffany (NJ) LLC v. Qi Andrew, et al.*, 276 F.R.D. 143, 159 (S.D.N.Y. 2011) (declining to compel production given conflict with Chinese banking statute, where history of prosecutions demonstrated that the 'statute has been used to prosecute individuals and that violations can result in serious punishment').

50 UK GDPR, Article 15.

51 European Data Protection Supervisor: 'Whistleblowing' available at https://edps.europa.eu/data-protection/data-protection/reference-library/whistleblowing_en.

In addition, under the UK GDPR, employees may demand any personal data held about them by their employer. This, the European Data Protection Supervisor has noted, is 'of particular concern in the whistleblowing context as it could, theoretically, risk exposing a whistleblower's identity'.[52] The Article 29 Working Party[53] stated that the right to access data may be restricted to ensure the whistleblower's rights are protected and '[u]nder no circumstances can the person accused in a whistleblower's report obtain information about the identity of the whistleblower from the scheme on the basis of the accused person's right of access, except where the whistleblower maliciously makes a false statement'.[54] This is reflected in the DPA 2018, which states that companies need not comply with a request for access to personal data if it would mean disclosing information about another individual who can be identified from that information, except if the individual has consented to the disclosure, or it is reasonable to comply with the request without that individual's consent.[55] Therefore, companies may be able to limit access to data following a whistleblower report, but they will still need to balance the data subject's right of access to personal data against the whistleblower's rights and the rights of any third parties mentioned in the report.[56]

See Chapters 19 to 21 on whistleblowers

Collecting, storing and accessing data: practical considerations 40.7

A few practical considerations for all investigations:

- Involve data controllers and other relevant organisations at as early a stage as possible.
- Identify any relevant documents to be transferred that contain special category data or any criminal offences data, and document the specific derogations or conditions on which that data will be used.
- Document all decision-making relating to the handling of that data (particularly any assessment of legitimate interests as a lawful basis for processing).
- Work with authorities to agree realistic expectations for the scope and timing of data requests.
- Consider all options for the transfer of data outside the United Kingdom or the European Union, including domestic review, redactions, MLATs and the use of domestic authorities, as well as the legal bases for transfer under GDPR; and document all decision-making relating to the international transfer of data.

52 ibid.

53 Now replaced by the EDPB.

54 Article 29 Data Protection Working Party, Opinion 1/2006, WP117 adopted 1 February 2006, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf.

55 DPA 2018, s.45.

56 European Data Protection Supervisor: 'Whistleblowing', available at https://edps.europa.eu/data-protection/data-protection/reference-library/whistleblowing_en.

Appendix 1

About the Authors of Volume I

Stuart Alford QC
Latham & Watkins

Stuart Alford QC is a partner in the London office of Latham & Watkins, and a member and former co-chair of the firm's litigation and trial department in London. Mr Alford advises leading corporations, high-growth companies, and financial institutions in a range of financial crime and regulatory matters, particularly corruption, money laundering and fraud, and in connection with shareholder disputes. Much of his work involves multiple jurisdictions and cross-border issues of investigation and competing laws.

From 2012 to 2016, Mr Alford headed the Fraud Division at the Serious Fraud Office (SFO), where he was responsible for many of the UK's landmark white-collar cases. His work focused on investigations in banking and money markets, including the wide-ranging cases involving the manipulation of LIBOR, foreign-exchange benchmarks and the Bank of England's liquidity auctions.

Mr Alford has extensive experience engaging with law enforcement and regulators around the world, including, in particular, the UK Financial Conduct Authority and the US Department of Justice. Mr Alford has significant experience managing parallel criminal and civil litigation, and has overseen significant data analysis projects and the advances in technology-assisted review and disclosure.

Before joining the SFO, Mr Alford spent 20 years in private practice as a barrister in London working in national and international criminal law. He was appointed Queen's Counsel in 2014.

Serrin A Turner
Latham & Watkins

Serrin Turner is a partner in the New York office of Latham & Watkins, where he is a member of the firm's data privacy and security practice, white-collar defence and investigations practice, and complex commercial litigation practice.

A former federal cybercrime prosecutor and experienced trial lawyer, Mr Turner represents technology companies and institutional clients in complex civil litigation, white-collar criminal defence matters, internal corporate investigations and crisis management situations, including data breaches and other cybersecurity incidents.

Gail E Crawford
Latham & Watkins

Gail Crawford, global chair of Latham's data and technology transactions practice, helps clients navigate complex data privacy and security matters, as well as to license, develop and exploit disruptive technology.

Ms Crawford advises many of the world's leading global technology companies on multifaceted and precedent-defining data privacy and security matters. Her work in the data privacy and security space encompasses advising on compliance programmes, product counselling, responding to data breaches and regulatory inquiries, advising on optimal organisational structures, and supporting large, strategic alliances and M&A transactions. She also helps clients navigate a myriad of issues in technology law, including commercial contracts, collaborations, and intellectual property.

Ms Crawford draws on her experience handling some of the most complicated and sensitive data privacy matters in the global market to provide pragmatic and commercially driven counsel. She brings a deep understanding of the innate value of data and the complex, ever-changing global regulatory framework to help clients achieve their business objectives.

Ms Crawford regularly writes and speaks on topics related to data privacy and disruptive technology, and serves as an editor of the Latham & Watkins Global Privacy & Security Compliance Law Blog.

Hayley Pizzey
Latham & Watkins

Hayley Pizzey is an associate in the London office of Latham & Watkins and a member of the firm's litigation and trial department.

Ms Pizzey is a trusted adviser to a number of international organisations. She is frequently engaged in complex and high-value disputes and regulatory inquiries. Ms Pizzey primarily handles multi-jurisdictional litigation and regulatory matters. She advises clients on a wide range of disputes, with a particular focus on commercial litigation and contentious data protection as well as regulatory investigations.

Ms Pizzey's role includes advising on inquiries commenced by the Irish Data Protection Commission, compliance with the GDPR, alleged data breaches and regulatory notifications, and regulatory sanctions.

Ms Pizzey's experience includes claims in the High Court, the Court of Appeal and the Competition Appeal Tribunal. She has also acted on matters involving the Competition and Markets Authority, the European Commission, and numerous data protection authorities and financial services regulators around the world.

Ms Pizzey is also a trusted adviser to her *pro bono* clients.

Mair Williams
Latham & Watkins

Mair Williams's practice focuses on white-collar defence. She has considerable trial experience, having started her career as a criminal barrister in chambers. She also has experience in investigations, representing companies and individuals before regulators and prosecuting bodies, and develops compliance policies and practices for international clients.

In addition to her white-collar work, Ms Williams has experience in all manner of complex commercial litigation and has represented clients at every stage, from initial pleadings to trial and appeal. She has worked with clients representing a full spectrum of industries, including financial services, media, food and beverage, manufacturing and technology.

Ms Williams has conducted a range of internal investigations in jurisdictions around the world, including an investigation of a financial services firm following a leak of confidential information to the media, and an investigation on behalf of a private pension scheme following allegations made by a whistleblower. Her diverse range of representative experience includes representing a director in an investigation by the Financial Reporting Council into discrepancies with annual accounts of a FTSE 250 company and representing a publicly listed investment firm in investigations by the Financial Conduct Authority and Serious Fraud Office.

Ms Williams is a passionate *pro bono* advocate, and her practice is focused on representing individuals in the criminal justice system, particularly post-conviction.

Matthew Valenti
Latham & Watkins

Matthew Valenti is an associate in the New York office of Latham & Watkins and a member of the firm's litigation and trial department. His practise focuses on white-collar defence and investigations, securities litigation, complex commercial litigation, and data privacy and cybersecurity issues.

Mr Valenti has represented individuals and corporations in a wide range of US government investigations led by the Department of Justice, the Commodity Futures Trading Commission, the Securities and Exchange Commission, and other regulatory agencies. He has also represented public and private companies in litigation in both federal and state court – including class actions alleging violations of US securities laws, and complex civil disputes implicating a broad spectrum of legal issues and industries. He also advises clients, both in regulatory inquiries and civil litigation, on data breach and data privacy matters.

Latham & Watkins

99 Bishopsgate
London, EC2M 3XF
United Kingdom
Tel: +44 20 7710 1000
stuart.alford.qc@lw.com
gail.crawford@lw.com
hayley.pizzey@lw.com
mair.williams@lw.com

1271 Avenue of the Americas
New York, NY 10020
United States
Tel: +1 212 906 1200
serrin.turner@lw.com
matthew.valenti@lw.com

www.lw.com

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-272-5