Global Investigations Review

The Practitioner's Guide to Global Investigations

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

Fifth 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

Fifth Edition

Editors

Judith Seddon

Eleanor Davison

Christopher J Morvillo

Michael Bowes QC

Luke Tolaini

Ama A Adams

Tara McGrath

GIR

Global Investigations Review

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK

www.globalinvestigationsreview.com

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at November 2020, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to:
natalie.hacker@lbresearch.com
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-272-5

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

ADDLESHAW GODDARD LLP

ANAGNOSTOPOULOS

ASSOCIATION OF CORPORATE INVESTIGATORS

BAKER MCKENZIE LLP

BCL SOLICITORS LLP

BDO USA, LLP

BORDEN LADNER GERVAIS LLP

BROWN RUDNICK LLP

CADWALADER, WICKERSHAM & TAFT LLP

CLARO Y CIA

CLIFFORD CHANCE

CLOTH FAIR CHAMBERS

COOLEY LLP

CORKER BINNING

CRAVATH, SWAINE & MOORE LLP

DEBEVOISE & PLIMPTON LLP

DLA PIPER LLP

FORNARI E ASSOCIATI

FOUNTAIN COURT CHAMBERS

FOX WILLIAMS LLP

FRESHFIELDS BRUCKHAUS DERINGER

GLEISS LUTZ

GOODWIN

GÜN + PARTNERS

HERBERT SMITH FREEHILLS LLP

HOMBURGER

JAMES P LOONAM ESQ

JENNER & BLOCK

KINGSLEY NAPLEY LLP

LATHAM & WATKINS

LAW OFFICES OF PANAG AND BABU

LINKLATERS LLP

MARVAL O'FARRELL MAIRAL

MATHESON

MAYER BROWN

MCGUIREWOODS

MISHCON DE REYA LLP

NAVACELLE

NORTON ROSE FULBRIGHT LLP

OUTER TEMPLE CHAMBERS

PHILIPPI PRIETOCARRIZOSA FERRERO DU & URÍA – PPU

PINSENT MASONS LLP

RAJAH & TANN SINGAPORE LLP

REBAZA, ALCÁZAR & DE LAS CASAS

REED SMITH LLP

ROPES & GRAY LLP

SKADDEN, ARPS, SLATE, MEAGHER & FLOM (UK) LLP

SLAUGHTER AND MAY

SOFUNDE OSAKWE OGUNDIPE & BELGORE

SULLIVAN & CROMWELL LLP

TRENCH ROSSI WATANABE

URÍA MENÉNDEZ ABOGADOS, SLP

VON WOBESER Y SIERRA, SC

WALDEN MACHT & HARAN LLP

WILLKIE FARR & GALLAGHER LLP

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 where the data protection regimes in different jurisdictions appear to be imposing 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 a company's 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 European General Data Protection Regulation (GDPR) – applicable in the United Kingdom until 31 December 2020 – and the UK Data Protection Act 2018 (DPA 2018). To prepare for Brexit and offer some continuity post-Brexit, the United Kingdom issued the UK General Data Protection Regulation (UK-GDPR), which contains no material differences to the GDPR. The UK government has also published a 'Keeling Schedule' to

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.

illustrate the differences between the GDPR and the UK-GDPR.[2] The provisions of the UK-GDPR will be incorporated directly into UK law from the end of the transition period (i.e., 31 December 2020), and will sit alongside the current DPA 2018 (as amended from the end of the transition period).[3] However, the EU version of the GDPR will continue to apply to UK companies if they operate, offer goods or services to individuals or monitor the behaviour of individuals in Europe.

UK laws governing the interception and monitoring of communications may also require navigation in the context of 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 €20 million or up to 4 per cent of annual worldwide turnover), and increased regulatory focus on data privacy, means that those conducting investigations must take the protections afforded to individuals more seriously than they did previously. The GDPR (which took effect on 25 May 2018) largely consolidated the previous European data protection regime and sought to harmonise the position within the European Union, 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, the GDPR not only catches EU corporations and global company groups with an EU presence (including their use of personal data outside the European Union to the extent that use is intrinsically linked with their EU activities), but also affects any corporations outside the European Union and with no EU presence that actively offer goods and services to, or monitor the behaviour of, individuals within the European Union, even if the data is stored outside it.

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 in the context of 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 GDPR's extraterritorial reach,[4] US and multinational companies may have to grapple with GDPR compliance obligations in conducting an internal investigation or responding to criminal or regulatory investigations. Where

2 https://www.gov.uk/government/publications/data-protection-law-eu-exit.

3 At the time of writing, a number of amendments to the DPA 2018 were to come into effect on 31 December 2020 to ensure the legislation functions correctly following the end of the transition period. The relevant Keeling Schedule can be found at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779334/Keeling_Schedule_for_Data_Protection_Act_2018.pdf.

4 The UK-GDPR will also have extraterritorial effect when it comes into force, meaning that US and multinational organisations may have to grapple with both GDPR and UK-GDPR compliance obligations in conducting an internal investigation or in responding to criminal, or regulatory investigations.

a US or multinational company's obligations to comply with US legal demands for personal data conflict with the GDPR's 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 GDPR. 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*.[5] 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 (an alternative to the EU-US Privacy Shield) to transfer personal data to the United States. If it cannot lawfully transfer responsive data to the United States, the US or multinational company 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 the context of criminal or regulatory investigations.[6]

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 GDPR and DPA 2018. For those conducting internal investigations, the key obligations to consider are (1) transparency, namely the requirement to inform individuals about how their personal data is being used (unless there is a relevant exemption), (2) data minimisation, namely the requirement to ensure that use of personal data for the investigation is proportionate, (3) establishing a legal basis for the processing of personal data, as prescribed by the 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), (4) 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 (5) if personal data will be transferred, or accessed from, outside the European Union, ensuring a legal basis for that data transfer, as prescribed by the GDPR (in addition to a legal basis for the underlying processing).

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

6 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); *United States v. First City Nat'l City Bank*, 396 F.2d 897 (2d Cir. 1968) (same).

Transparency 40.2.1

The 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.[7] This forms part of the wider GDPR principles of transparency and fairness, which seek to prevent organisations from using data in ways that are detrimental, unexpected or misleading to individuals. Meeting these obligations in the context of 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. (The exemptions do not apply to the requirements to process personal data transparently and fairly.) When collecting personal data directly from an individual, organisations are not required to 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 in the context of internal investigations apply if providing the information to the individual would be impossible or would involve disproportionate effort; providing the information to the individual 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 (which necessitates 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 GDPR, the UK's regulatory framework for communications monitoring also requires organisations to be transparent with employees about the interception and monitoring of their communications (both in written policies and also in consistent business practices). Taken together, in the context of internal investigations, the data protection and communications regimes oblige organisations to be clear and open with employees about how their personal data and their communications are used, and to ensure that any interception and subsequent review, use and disclosure of data and communications in an investigation is both lawful and proportionate. Robust, clear and accessible data privacy information notices for employees, as well as policies on employee monitoring, will provide a valuable shield against claims of

7 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 EU and applicable data retention periods.

employee privacy infringement and non-compliant monitoring practices – at least in the United Kingdom.[8]

40.2.2 Data minimisation

The 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 key word searches and time periods to identify relevant information, etc.).

40.2.3 Legal basis for data processing: consent

Consent from the individual provides a legal basis for the processing of that individual's personal data, provided the GDPR consent conditions are met. The GDPR establishes a higher standard for consent for the processing of personal data than the Data Protection Act 1998 (DPA) it replaced.[9] 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.

In the typical employer–employee context of an internal investigation, the concept of consent being freely given is a complicated one. Given the dynamic, some jurisdictions consider that consent from an employee to an employer may never be freely given,[10] 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 with the 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

8 The position in a number of other 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.

9 GDPR, Article 7 and Recital 32.

10 The European Data Protection Board's Guidelines on consent under the 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.

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 one of the other lawful bases under the GDPR (discussed below) to lawfully process the data.

Legal basis for data processing: legitimate interest 40.2.4

The GDPR provides a number of other legal bases for the processing of personal data in certain circumstances.[11]

Under the 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.[12]

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 UK's 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 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. In respect of the necessity test, companies must consider whether there is an alternative, less intrusive, means of gathering or processing the same information.

To demonstrate compliance with the GDPR, organisations will have to document their decisions carefully (through a legitimate interests assessment).[14]

11 GDPR, Article 6.

12 This provides additional flexibility to data processors; under the DPA, third-party interests were restricted to those third parties to whom the data would be disclosed.

13 'Legitimate interests' (Information Commissioner's Office): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.

14 Ibid.

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[15] (which replaces the 'sensitive personal data' terminology under the DPA, and expands the categories of personal data subject to additional restrictions). 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. The concept of special category data is dealt with under Article 9 of the GDPR (and section 10 of the DPA 2018) and it has been extended to include genetic and biometric data.

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 GDPR) and an additional, specific legal basis for processing the relevant special category data. The GDPR and DPA 2018 provide for a number of specific legal bases or conditions for the use of special category data, the most relevant of which for internal investigations are consent of the individual (specifically to the use of his or her special category data), processing for the purposes of establishing or defending a legal claim, and public interest purposes as specifically provided for in national law.

Information about criminal allegations, proceedings or convictions in relation to an individual may also be relevant in the context of an internal investigation. This data is treated separately under the GDPR, and requires a lawful basis for processing and legal or official authority to handle that data, which must be specifically prescribed under national law. In the United Kingdom, the DPA 2018 authorises the processing of criminal offences data in certain limited circumstances and subject to the conditions set out in the DPA 2018.[16] These legal authority grounds are narrow, though certain grounds may be available in internal investigations, including prescribed public interests 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 Special category data is defined in the 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' (Article 9 of the GDPR and section 10 of the DPA 2018).

16 DPA 2018, Part 1 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. However, 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'.[17] Both provisions require that processing be done without consent of the individual, to avoid prejudicing the investigation. The scope of the public interest ground for data processing under the GDPR must be provided for under national law, and may vary across the European Union. Organisations should therefore seek local legal advice in the relevant Member States.

Data transfer outside the 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 GDPR. If the personal data will be transferred, or accessed from, outside the 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 GDPR, in addition to the lawful processing of the data itself. This restriction on data transfers does not apply to non-EEA countries recognised as 'adequate' by the European Commission, to which personal data may be transferred freely.[18] On 16 July 2020, in the *Schrems II* decision, the CJEU invalidated the European Commission's EU-US Privacy Shield Adequacy Decision (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.[19] In the same judgment, the CJEU ruled that the standard contractual clauses (SCCs)[20] (an alternative to the EU-US Privacy Shield as a data transfer mechanism) remain valid in respect of any personal data export (not just EEA-US transfers), but imposed significant caveats on their use.

17 Ibid., at Schedule 1, Part 2.

18 Currently, Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay are recognised as having adequate protection. Adequacy talks with South Korea are ongoing.

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

20 Sometimes referred to as the 'Model Clauses'.

Investigations involving data transfers to countries or entities outside the EEA and not recognised as 'adequate' (which, following *Schrems II*, includes US organisations certified under the now-invalidated EU-US Privacy Shield) will require other grounds or safeguards to enable the transfer, as set out in the GDPR. The safeguard most commonly relied on in this context, 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 data importing entities.[21] Many international organisations are likely to be familiar with the SCCs as part of their wider data privacy compliance efforts. However, the CJEU in the *Schrems II* decision imposed a number of caveats on the use of the SCCs. Organisations seeking to rely on the SCCs are required to 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 additional safeguards to ensure an essentially equivalent level of protection. In relation to data transfers to the United States specifically, the CJEU found that, in its judgement, the US legal regime does not ensure 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. The European Data Protection Board (EDPB) subsequently stated that the SCCs can therefore only be used to transfer personal data to the United States, provided appropriate supplementary measures are put in place to ensure that US laws do not impinge on the level of protection guaranteed by the SCCs.[22] The EDPB also suggested that, if an organisation's assessment of the data transfer concludes that the data is not adequately protected, yet the organisation intends to continue with the data transfer nonetheless, the organisation should notify the relevant supervisory authority. While it remains to be seen how European data protection authorities will enforce the requirements of the *Schrems II* decision in practice, organisations should carefully consider use of the SCCs to validate data transfers to the United States in the context of internal investigations, and to document any assessments.

There are alternatives to the SCCs under the GDPR, 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).

In the event of a no-deal Brexit, the GDPR rules on data transfers will be mirrored into UK law. Therefore, personal data transfers from the United Kingdom will be subject to similar restrictions and requirements, except in relation to transfers to EEA Member States, which can continue. The requirements for data transfers from the United Kingdom to countries outside the EEA will remain similar

21 The current versions of the SCCs can be accessed at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

22 EDPB Schrems II FAQs, which can be accessed at https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf.

to current GDPR rules, and the UK government has confirmed that it intends to recognise existing EU adequacy decisions and approved SCCs wherever possible. In relation to transfers from the EEA to the United Kingdom, the GDPR's data transfer rules will apply to restrict those data transfers, unless and until an adequacy decision is granted by the European Commission in favour of the United Kingdom. The UK government has applied for an adequacy decision, which, if granted, would allow personal data to be transferred freely from the EEA to the United Kingdom – though such a decision will inevitably take time to be negotiated and granted, and the outcome is not currently clear.

Different data transfer considerations apply in the context of 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 very often require access to personal data in order to act. The GDPR has introduced new requirements when entering into such arrangements, which means that a contract or other legal act under European Union or Member State law is now required where controllers engage the services of processors.

This 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 certain prescribed contractual obligations.[23] The GDPR changed the required clauses, so it is particularly important to ensure that the correct agreements are in place from the outset of any interaction with third parties. In addition, any agreement must contain an obligation of confidentiality.[24]

Monitoring employees' electronic communications 40.2.9

In addition to the data protection considerations discussed above, 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.[25] These communications regulations are triggered on '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 the context of internal investigations,

23 GDPR, Article 28(3).

24 Ibid., at Article 28(3)(a) to (h).

25 This framework consists primarily of the Regulation of Investigatory Powers Act 2000 (RIPA); the Investigatory Powers Act 2016 (IPA 2016), which updates and repeals certain parts of RIPA; the Interception of Communications Code of Practice under the IPA 2016; and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (Lawful Business Practice Regulations), which were enacted under RIPA but have not to date been replaced or repealed by the IPA 2016.

this will most likely be of relevance when considering investigation-specific interception and monitoring of employee communications, or when assessing the legality of an organisation's existing 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 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.[26] If consent is relied on for interception purposes, this should be distinguishable from any consent relied on for 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 been brought against employers in the context of searches in the workplace.[27] While courts have typically upheld an employer's right to search company-owned property, including computers and devices, there is no bright-line rule. In cases involving more unusual facts, an employee may be able to make out an invasion of privacy claim based on a workplace search.[28] 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. An employee will face

26 Provided for under the Lawful Business Practice Regulations and the Communications Code of Practice.

27 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).

28 See, e.g., *Doe v. Kohn Nast & Graf*, 866 F. Supp. 190 (E.D. Pa. 1994) (allowing an invasion of privacy case to proceed to jury based on a company's opening of mail sent to the workplace that appeared to be personal in nature); *Rene v. G.F. Fishers, Inc.*, 817 F. Supp.2d 1090 (S.D. Ind. 2011) (allowing claims under the Stored Communications Act (SCA) and the Indiana Wiretap Act to survive where a company decoded the employee's passwords to personal accounts which had been accessed on company computers).

difficulty establishing a right to privacy in company-controlled systems or data where such policies are in place.[29]

Other state laws place more specific prohibitions on employers that can limit the outer bounds of a company's investigative actions. For example, various state laws prohibit questioning an employee on issues that serve no business purpose,[30] demanding an employee disclose passwords and other credentials to his or her personal email and social networking accounts,[31] requiring employees to alter privacy settings on their electronic accounts,[32] or asking employees to access social media accounts in the presence of the employer.[33]

29 See, e.g., *Leventhal v. Knapek*, 266 F.3d 64 (4th Cir. 2000) (finding no legitimate expectation of privacy in internet use when an employer's known policy allowed monitoring of 'all file transfers, all websites visited, and all e-mail messages'); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (holding that employees did not have an 'objectively reasonable expectation of privacy' in email messages stored on computer network); *Garrity v. John Hancock Mut. Life Ins. Co.*, 2002 U.S. Dist. LEXIS 8343, at *5 to 6 (D. Mass. 7 May 2002) (that an employer instructed its employees on creating personal passwords for their computers did not create reasonable expectation in privacy); *Muick v. Glenayre Elecs.*, 280 F.3d 741 (7th Cir. 2002) (employee did not have reasonable expectation of privacy in his company-owned laptop); *Thygeson v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 18863 (D. Or. 15 September 2004) (employee had no reasonable expectation of privacy in websites accessed on work computer where company had a policy regarding personal computer use and monitoring); *Garrity v. John Hancock Mutual Life Insurance Co.*, 2002 U.S. Dist. LEXIS 8343 (D. Mass. 7 May 2002) (the employee had no reasonable expectation of privacy in emails transmitted on an employer's computer system where the employer's interest in preventing sexual harassment was greater than the employee's privacy interest); Restatement (Third) of Emp't Law § 7.03 (Council Draft No. 6, 2011). ('[A] clear employer notice or policy that a particular location is not private for employees generally defeats an employee's expectation of privacy, unless the employer's actual practices contravene the wording of an express notice or policy.'); *O'Connor v. Ortega*, 480 U.S. 709, 713 (1987) (plurality opinion) (stating that a government employee had a reasonable expectation of privacy in his desk and file cabinets where 'there was no policy of inventorying the offices of those on administrative leave' and 'there was no evidence that the Hospital had established any reasonable regulation or policy discouraging employees such as Dr Ortega from storing personal papers and effects in their desks or file cabinets').

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 See, e.g., 26 M.R.S.A. § 615.

33 Id.; see, e.g., Cal. Lab. Code § 980 (2012) (allowing an employer to require an employee to 'divulge personal social media reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations,' but information must be used solely for the investigation); 820 Ill. Comp. Stat § 55/10 (2012) (granting an employer the ability to require employees to share specific content of personal online accounts (but not user name and passwords) that has been reported to the employer for purposes of investigating employee misconduct); Wash. Rev. Code § 49.44.200 (2013) (permitting an employer to require an employee to share content (but not the login information) from his or her social media account as necessary to comply with applicable laws or investigate employee misconduct).

Various state and federal laws also restrict the collection of electronic communications, including emails[34] (both work and personal), phone calls[35] and social media accounts.[36] One primary federal law is the Electronic Communications Privacy Act,[37] which breaks down into the Wiretap Act (which generally prohibits intercepting electronic communications),[38] the Pen Register Statute (which generally prohibits use of a pen register to track communications)[39] and the Stored Communications Act (which generally prohibits unauthorised access to stored electronic communications).[40] These statutes do not generally prohibit an employer from searching its own email system.[41] 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),[42] 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

34 See *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).

35 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, -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).

36 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).

37 See 18 U.S.C. §§ 2510-22, 2701-12.

38 Id., at §§ 2511-2522.

39 Id., at §§ 3121-3127.

40 Id., at §§ 2701-2711.

41 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).

42 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).

the Illinois Biometric Information Privacy Act (BIPA).[43] BIPA defines biometric information broadly to include 'any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual'.[44] Employers who intend to use such biometric information for any purpose, including for time management, security access or safety, must first obtain informed written consent prior to collection.[45] Employers can obtain consent via an employment agreement.[46] A failure to obtain proper consent, among other things,[47] can result in potential exposure to liability,[48] as the Illinois Supreme Court has ruled that any violation of the law – regardless of the presence of particularised harm – confers standing on the affected individual to sue for potentially substantial statutory damages.[49]

Finally, besides state and federal laws, internal investigations in the United States may also be subject to the GDPR's restrictions,[50] given its extraterritorial reach. In particular, to the extent the investigation requires review of personal data stored in the European Union – for example, an employment file for an employee in an EU affiliate, stored on a server in the European Union – then the company must evaluate whether (1) the EU company 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 above 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 European Union, or redacting personal information from the data set before it is transferred.

43 740 ILCS 14/1 (2008).

44 Id., at § 10.

45 Id., at § 15.

46 Id., at § 10 ('"Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.')

47 BIPA also regulates the disclosure, protection and retention of, as well as profiting off of, biometric information by employers. See id., at § 15.

48 Id., at § 20 (BIPA provides for a privacy right of action).

49 See *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 34 (Ill. 2019) ('When a private entity fails to adhere to the statutory procedures . . . the right of the individual to maintain his or her biometric privacy vanishes into thin air. . . . The injury is real and significant.' (internal quotations and modifications omitted)); see also *Patel v. Facebook*, 18-15982 (9th Cir. 8 August 2019) (holding that plaintiffs sufficiently alleged Article III standing to bring BIPA claims because 'an invasion of an individual's biometric privacy rights has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts') (internal citation and quotation marks omitted).

50 And the UK-GDPR from 1 January 2021.

40.4 Investigations by authorities: UK perspective

Companies have always had to consider competing interests when dealing with investigating authorities, but, until recently, data protection has rarely been near the top of any list of considerations. The very significant fines available under the GDPR mean that companies must take data protection much more seriously, particularly the disclosing of personal data to authorities both in the United Kingdom and overseas. The ICO has shown that it will not hesitate to use its powers under the GDPR to investigate and issue significant fines for breaches. For example, on 8 July 2019, the ICO announced a notice of intent to fine British Airways £183.39 million[51] for a data breach affecting 500,000 individuals brought about by 'poor security arrangements'.[52] This was closely followed by a further notice of intent to fine on 9 July 2019 whereby the ICO is proposing to fine Marriott International £99.2 million[53] for infringements of the GDPR stemming from a data breach at Starwood, which Marriott acquired in 2016, effecting 300 million individuals.[54] On 17 December 2019, the ICO issued its first fine under the GDPR to a London-based pharmacy, Doorstep Dispensaree Limited, for £275,000[55] for failing to ensure the security of special category data.[56] It remains to be seen whether this initially robust approach to GDPR enforcement from the ICO will extend into the more nuanced environment of internal and regulatory investigations, with their frequently competing legal obligations.

40.4.1 Guidance from authorities

Prior to the introduction of the GDPR, concerns were raised about the balance companies should strike between their reporting and regulatory commitments (including investigations), on the one hand, and protecting their employees' (or anyone else's) personal data on the other. To offer some guidance in this regard, the Financial Conduct Authority (FCA) and ICO published a joint update on the GDPR in which they made clear that they believed 'the GDPR does not impose requirements which are incompatible with the rules in the FCA Handbook'.[57]

51 1.5 per cent of British Airways 2017 global revenue.

52 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/.

53 2.5 per cent of Marriott's 2017 global revenue.

54 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

55 While Doorstep Dispensaree's revenue is not publicly available, its filed accounts indicate it is a 'small company' under the UK Companies Act 2006. This means it satisfied any two of the following criteria: (1) turnover not more than £10.2 million; (2) balance sheet total of not more than £5.1 million; and (3) not more than 50 employees. Assuming Doorstep Dispensaree satisfies the annual turnover criteria (i.e., £10.2 million or less), the ICO's fine could equate to 2.6 per cent of Doorstep Dispensaree's annual revenue. While at first blush the fine may appear small, it could indicate further significant enforcement action by the ICO.

56 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/12/london-pharmacy-fined-after-careless-storage-of-patient-data/.

57 https://www.fca.org.uk/news/statements/fca-and-ico-publish-joint-update-gdpr.

Further, the FCA and ICO have published a memorandum of understanding,[58] which (among other things) pledges each regulator to seek to understand and, where appropriate, collaborate and co-ordinate work on their respective policies that have a material effect on the other's objectives. This is yet to be tested and it is unclear whether the FCA will be tolerant of delays, limitations on information and other issues caused by a company's cautious approach to data protection.

Furthermore, the FCA has been keen to point out that it will be considering breaches of the GDPR as part of its supervision of senior management arrangements, systems and controls.[59] Although this is limited to entities regulated by the FCA, it seems likely that other authorities will take a similar approach and companies will need to be ready to show that they have taken their data protection obligations seriously – whether they are ongoing, part of an investigation or a data request from an investigating authority.

Providing data to authorities 40.4.2

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 GDPR obligations. The benefits of voluntarily handing over more data than specifically required have probably disappeared with the GDPR's tougher data regulation regime. Among other things, the 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 EEA. These obligations apply equally in the context of 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 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 national UK or European law. Obligations originating from outside the United Kingdom or Europe do not provide a legal basis for data processing on this ground, even where those obligations may be binding on a non-European 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 GDPR compliance.

In the context of international investigations, companies will need to address the GDPR restrictions and requirements for the transfer of personal data outside the EEA. The considerations for organisations disclosing data to third party

58 https://ico.org.uk/media/2614342/financial-conduct-authority-ico-mou.pdf.

59 https://www.fca.org.uk/news/statements/fca-and-ico-publish-joint-update-gdpr.

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 GDPR requirements for transferring data under international agreements, such as mutual legal assistance treaties (MLATs).[60] 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 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.[61]

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

Some national regulators (such as the FCA 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 GDPR and so may not be an appropriate method for data transfer. While the interpretation of Article 48 of the 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 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 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 GDPR, but undue redaction may not be welcomed by the receiving authorities.

60 GDPR, Articles 48 and 49.

61 The UK-US Bilateral Data Access Agreement was signed on 3 October 2019, and allows law enforcement authorities in the United States and the United Kingdom 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.

Investigations by authorities: US perspective 40.5

As in the United Kingdom, companies in the United States must be mindful of the GDPR's 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. It is common for US law enforcement agencies or regulators to issue demands for documents to companies requiring the production of large volumes of data. To the extent that responsive data is stored in the European Union, and contains personal data subject to the 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's restrictions.

A US company concerned that it faces such 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 GDPR-regulated data. This is particularly important because, for the company to rely on the GDPR's legal defence derogation to produce the data to US authorities, the data must be '*necessary* for the establishment, exercise or defence of legal claims'.[62] Accordingly, obtaining clarity from law enforcement or the regulatory agency as to what personal data is necessary to respond to the request, and redacting or otherwise anonymising the other personal data that is not needed, will put a company in a more defensible position if GDPR issues arise.

At the same time, US law enforcement authorities or regulatory agencies are likely to press for clarity as to whether the GDPR genuinely prohibits the transfer of the data in question to US authorities. The US Department of Justice has taken a robust approach previously in similar circumstances, by asserting: 'Where 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.'[63] Although the risk of breaching obligations under the GDPR 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 GDPR's transfer restrictions, and the company is unable to negotiate an adequate resolution with the US authorities involved, 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

62 Ibid., at Article 49.

63 https://www.justice.gov/archives/opa/blog-entry/file/838386/download.

on international comity. If the court agrees that compliance with the demand for documents would give rise to a true conflict of laws, it will weigh the conflicting legal obligations of US law and foreign laws case by case.[64] Specifically, a court entertaining such a challenge must consider, among other things, the importance of the records to the US legal matter for which they are sought, the availability of alternative means of securing the information and the extent to which non-compliance with the request would undermine important interests of the United States, or compliance would undermine important interests of the state where the information is located.[65]

However, while courts have sometimes quashed subpoenas on comity grounds in civil litigation,[66] they have typically rebuffed such challenges in the context of criminal investigations, finding that the domestic interest in enforcing the criminal laws trumped the foreign data privacy interests involved.[67] The enforcement of the GDPR and the severe potential penalties that attach to non-compliance may provide greater motivation to companies to challenge US legal process if they believe there is a risk that compliance will run afoul of the GDPR's requirements; and likewise, the prospect of GDPR penalties may lead US courts to give more weight to foreign data privacy interests than they might otherwise in such challenges. Indeed, US court decisions applying the international comity balancing test have sometimes turned, in significant part, on the low likelihood of severe penalties being imposed on the recipient of the legal process at issue if complied with.[68] It is unclear, however, whether and to what extent the GDPR will actually change the equation in this regard – at least prior to a significant fine or other penalty for a disclosure.

64 *Linde v. Arab Bank, PLC*, 706 F.3d 92, 108 (2d Cir. 2013).

65 See *Société Nationale Industrielle Aérospatiale v. United States Dist. Court for S. Dist.*, 482 U.S. 522, 544 n.28 (1987); see also Clarifying Lawful Overseas Use of Data Act (2018), P.L. 115-141 (amending section 2523 of the SCA and codifying the common law comity challenge with respect to compelled process for data served pursuant to the SCA).

66 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. May 23, 2012).

67 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); *United States v. First City Nat'l City Bank*, 396 F.2d 897 (2d Cir. 1968) (same).

68 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').

Whistleblowers 40.6

The interplay between the increased protections for individuals under the GDPR and the protections for whistleblowers under existing laws is a particularly interesting one 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.

Whistleblowing policies and data protection 40.6.1

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

Right to access 40.6.2

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.[69] The personal information in a whistleblowing report can relate to whistleblowers, the persons under investigation, witnesses or other individuals that are mentioned, meaning that companies will need to uphold the data protection rights of all involved.[70]

In addition, under the 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'.[71] The Article 29 Working Party (now replaced by the European Data Protection Board) has stated that the right to access data may be restricted in order 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

69 GDPR, Article 15.

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

71 Ibid.

whistleblower maliciously makes a false statement'.[72] This is reflected in the DPA 2018, which states that companies do not have to 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 other individual has consented to the disclosure, or it is reasonable to comply with the request without that individual's consent.[73] 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 their personal data against the whistleblower's rights and the rights of any third parties mentioned in the report.[74]

See Chapters 19 to 21 on whistleblowers

40.7 Collecting, storing and accessing data: practical considerations

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) and any transfer of that data outside the United Kingdom or the European Union and consider it against Article 49 of the GDPR.
- 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.

72 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.

73 DPA 2018, Section 45.

74 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, as well as 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.

Ms Pizzey is a trust 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 across the world.

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

Mair Williams
Latham & Watkins

Mair Williams' practice focuses on white-collar defence. She has considerable trial experience having started her career as a criminal barrister in chambers, as well as experience in investigations, representing companies and individuals before regulators and prosecuting bodies, and developing 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 through to trial and appeal. She has worked with clients from 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 across 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 a number of individuals and corporations in a wide range of 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

885 Third Avenue
New York, NY 10022-4834
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

an LBR business

ISBN 978-1-83862-272-5