Chapter V:
Data Privacy & Blocking Statutes

Summary

Key Principles:

— ***Broad scope***: The concept of what constitutes processing of personal data under European law is extremely broad.

— ***Processing requirements***: Personal data must be processed in accordance with principles of lawfulness, fairness, transparency, purpose limitation, data minimization, integrity, confidentiality, and accountability. Lawful processing requires consent or another legal basis provided for in EU or member states' national law. This can significantly limit a company's ability to produce personal data in the event of an investigation or other crisis.

— ***Employee monitoring***: More stringent restrictions apply to the processing of personal data in an employment context, especially when processing sensitive data.

— ***Transfer outside the EU***: Except in a limited number of circumstances, the transfer of personal data outside of the EU is only allowed to countries or organizations offering adequate protection, based on a decision of the European Commission, other appropriate contractual safeguards, or binding rules. Transfers to comply with a decision or order by a foreign court or administrative body require additional scrutiny.

Being Prepared:

— Identify all relevant jurisdictions where personal data is stored or processed and evaluate the legal grounds relied on for processing and transferring personal data.

— The GDPR has introduced significant changes, including with respect to transparency and consent requirements, data subjects' rights, regulatory oversight, and enforcement. Review data protection policies, monitoring policies, codes of conduct, and personal data inventories to ensure compliance and mitigate risks.

  - Include compliance and investigative processes as express purpose for data collection in privacy notices and internal policies.
  - Create robust ediscovery protocols and obtain the necessary approval such as from works council to simplify the process at the time of an investigation.
- Maintain a data privacy investigations and productions protocol, and be prepared to consult with local counsel as needed.

Introduction

In this chapter, we address data privacy and blocking statutes in two jurisdictions likely to be critical in any global crisis, the European Union ("EU") and Switzerland. Because these statutes raise complicated issues relating to the ability to process and transfer data, it is critical to consider these issues ahead of time, and to be prepared by taking certain pre-emptive steps designed to facilitate compliance with the rules and better position the company in the event of a crisis. Moreover, because the EU's new General Data Protection Regulation only went into effect in May 2018, it is important for companies to continue to update their analysis of the application of these statute as new guidance is provided by the authorities.

General Principles

Protection of personal data as a distinct fundamental right

In the European Union ("EU") both the right to respect each person's private life, home and communication ("privacy") and the right to the protection of personal data are recognized and protected as a fundamental individual rights. Article 7 of the EU Charter of Fundamental Rights (the "Charter") of 2000 protects the right to privacy and Article 8 of the Charter has elevated the protection of personal data to a specific and distinct fundamental right in the European Union and provides that the processing of personal data is prohibited, unless based on a legitimate basis

found in the law.[1] This fundamental right has also been repeatedly emphasized by the Court of Justice of the European Union ("CJEU").[2]

Until May 25, 2018, data protection within the European Union was governed by Directive 95/46/EC, adopted in 1995 (the "Directive")[3], which also established the advisory Article 29 Data Protection Working Party. As a directive under EU law, it left the implementation of the legal framework to the individual member state legislators[4], causing national data privacy laws in the European Union to have deviated to a certain extent.

Reform – GDPR

That situation changed as of May 25, 2018. On that date, the General Data Protection Regulation (EU) 2016/679 ("GDPR") replaced the Directive. As a regulation, it is binding in its entirety and directly applicable across all EU member states without the need for further national or local implementing implementation.[5] Although the general principles of the GDPR are broadly in line with the previously applicable legal regime, we will throughout this chapter highlight certain key differences and new concepts that need to be taken into consideration by companies that are active within the territorial scope of the GDPR. The GDPR also grants broader powers to the supervisory authorities, including the capacity to impose higher fines. For example, failure to ensure appropriate security of personal data or transferring personal data outside of the EU in violation of the GDPR can attract a fine of up to the higher of EUR 20 million or 4% of a company's total worldwide annual turnover.[6] As a result, companies must ensure compliance with the GDPR in connection with

---

1 Article 8(2) of the Charter.

2 CJEU Case C-553/07, *Rijkeboer*, EU:C:2009:293, § 47; C-291/12, *Schwarz*, ECLI:EU:C:2013:670; Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Others*, EU:C:2014:238, § 53; Case C-131/12, *Google Spain and Google*, EU:C:2014:317, §§ 53, 66 and 74; C-362/14, *Schrems*, ECLI:EU:C:2015:650; Joined Cases C-203/15, *Tele2 Sverige AB* and C-698/15, *Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

3 Directive 95/46/EC of the European Parliament and of the Council of October 24, 1994 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

4 Article 288 of the TFEU: "*a regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States*" and "*a directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.*"

5 Even though the GDPR leaves room for further implementation measures at national level in certain areas such as employment and processing of personal data of minors.

6 Article 83(5) GDPR. See also the Cleary alert memo on GDPR: The General Data Protection Regulation: Key Changes and Implications (https://www.clearygottlieb.com/~/media/organize-archive/cgsh/files/publication-pdfs/alert-memos/alert-memo-pdf-version-201650.pdf).

the transfer of any data, or risk significant penalties (although it remains to be seen how the GDPR is enforced in practice, of course).

Scope of Application of Data Privacy Rules

Broad Scope

The concept of "processing[7]" of data under European law is extremely broad and includes any action performed on that data, including, for example, merely storing it beyond the regular data retention, such as for a litigation hold.[8] What qualifies as personal data[9] may be as simple as an individual's name or email address (including business email), but may of course also encompass more sensitive information, which can trigger an even higher standard of protection.[10] Accordingly, European data privacy rules will apply to many of the actions necessary for an internal investigation or for responding to requests from public authorities in the event of a crisis, such as collecting data and reviewing it as part of an investigation.

The primary responsibility for compliance with data privacy laws when personal data is being processed resides with the "controller"[11], defined as "*the natural or legal person* [...] *which, alone or jointly with others, determines the purposes and means of the processing of personal data*." In the context of an internal investigation for example, the controller will usually be the company performing the investigation. When responding to governmental inquiries, it may become less clear who the

[7] Processing is defined as "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*" (Article 2(b) Directive). Under GDPR, this definition will be slightly expanded to also cover structuring and restricting access to personal data (Article 4(2) GPDR).

[8] European data privacy laws apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system (Article 2 GDPR). Data processing by public authorities themselves for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security, is generally carved-out from the scope of the applicable privacy rules (Article 2(2) lit. d GDPR and future Directive (EU) 2016/680). But this carve-out does not apply to companies performing an internal investigation or cooperating with such public authorities.

[9] Personal data is defined as "*any information relating to an identified or identifiable natural person; an identifiable natural person or "data subject" is one "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*" (Article 4(1) GDPR).

[10] Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life are considered sensitive (Article 8(1) Directive). Under GDPR, this definition will be expanded to also cover genetic and biometric data (Article 9(1) GDPR).

[11] Note that unlike the current regime of the Directive, the GDPR does contain specific statutory obligations for processors, who will face directly liability concomitantly with the controller.

controller is, as many different actors can become involved and those entities may hold joint controllership.

Other parties typically involved in an investigation, such as external consultants and, under certain circumstances, even legal counsel supporting an internal investigation or the preparation of a response to regulator, will often be considered a "processor"[12], acting on behalf of the controller. The controller is not exonerated from liability under data privacy laws because the violation was committed by a processor on behalf of a controller. Data processors also have (increased) responsibility under the GDPR as, unlike with the Directive, the GDPR imposes direct legal compliance obligations on processors.[13]

DOCUMENTING PROCESSING BY EXTERNAL SERVICE PROVIDERS

Companies should be prepared to negotiate the legal terms and conditions of data processing agreements with external data processors, in particular in light of limitations of liability and hold harmless provisions concerning possible breaches of applicable data privacy laws. EU data privacy laws require that the relationship between the data controller and a data processor is governed by a binding written contract that sets out, among others, the subject-matter and duration of the data 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 parties in relation to the processing in sufficient detail.[14]

Territorial Scope

Unlike the Directive, which applied to processing carried out by companies either (i) established in an EU member state[15] or (ii) using equipment based in the EU, the GDPR has a significantly broader scope of application. The GDPR will apply extraterritorially to any internal investigation or preparation of a response to governmental requests that involves the processing of personal data of individuals who

[12] A "processor" is defined as "*a natural or legal person, public authority, agency or any other body which processes personal data* ***on behalf of the controller***" (emphasis added).

[13] Article 3 GDPR. These additional responsibilities for data processors include the implementation of technical and organizational measures, promptly notifying the data controller of any data breaches, and informing the data controller if the processor believes the instructions received from the controller are not GDPR-compliant.

[14] Article 28 GDPR.

[15] Or in a place where a member state's law applies by virtue of public international law.

are present in the EU, where the processing activities are related to monitoring of their behavior within the EU, irrespective of whether the company or data processor is established in the EU or whether or not the processing activities are performed in the EU.[16]

Processing Personal Data

What are the requirements for the processing of personal data?

Requirement of a legal basis

Personal data must be processed "l*awfully, fairly and in a transparent manner in relation to the data subject*".[17] A company processing personal data for purposes of conducting an internal investigation or responding to a governmental inquiry must ensure that a legal basis exists in order for it to be in complicate with data protection laws. The GDPR provides an exhaustive list of available legal bases, including consent by the data subject, compliance with a legal obligation, or performing a task carried out in the public interest, and the "legitimate interests" of the controller.[18]

Parties often gravitate towards consent from the relevant data subjects to justify processing as the seemingly simplest solution. However, this is often not the most expedient approach in the context of internal investigations or regulatory inquiries[19] because the requirements for consent are high and, even after consent is obtained,

[16] More broadly, the GDPR will apply to all controllers or processors established within the EU and processing personal data in the context of the activities, regardless of whether the data processing takes place in the EU or not (see also Article 3 GDPR).

[17] Article 5(1)(a) GDPR.

[18] See Article 6(1) GDPR, which broadly replicates the permissible grounds of the Directive. A legal basis exists if one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Member States may introduce specific provisions providing a legal basis for processing under national law. For companies processing "sensitive" personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, and genetic and biometric data, additional restrictions apply and the list of permissible grounds is even shorter, cf. Article 9 GDPR.

[19] It may often be impossible to contact all data subjects for practical or confidentiality reasons. Moreover, consent in the employer-employee context is seen as problematic by European Data Protection Authorities due to the imbalance of power inherent in the relationship, which calls the voluntary nature of such a consent into question. That consent must be freely given is however a key component. (See Article 29 Working Party, WP 249, 21).

it can be withdrawn by the data subjects at any time.[20] This would make any further processing unlawful and may also require the deletion of data that has already been processed.

Data processing by private entities in the context of investigations could be considered necessary either "f*or the performance of a task carried out in the public interest*" or "*for compliance with a legal obligation to which the controller is subject*".[21] The GDPR specifically mentions data exchanges in the context of competition law oversight, tax or customs administration, and financial supervisory authorities, and it is conceivable that cooperation in the context of an investigation with such global scope (such as the investigations relating to LIBOR, for example) could be considered to be in the public interest even for data transfers from private entities. However, the GDPR provides that these legal bases are narrowly interpreted. For example, the "legal obligation" has to be found in EU or member state law and could not for instance be based on a "*unilateral decision by a third country*," which suggests that responding to a subpoena from an authority outside of the EU, by itself is not a sufficient basis to process the data.

Outside of these exceptions, data processing may be permitted to the extent it falls within the company's "legitimate interests". To rely on this ground, the processing of personal data must be "*necessary for the purposes of the legitimate interests pursued by the company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data* [...]."[22] Whenever relying on this amorphous legal basis, companies must perform and document a true weighing and balancing of on the one side, their legitimate interests in processing personal data for compliance or investigative purposes (e.g., ensuring compliance with laws and/or avoiding civil or criminal sanctions, liability, negative publicity) and, on the other side, the fundamental rights of the individuals whose data is being processed (e.g., their right to privacy

[20] For guidance and analysis of the notion of consent under GDPR, see also Article 29 Working Party, WP 259, Guidelines on Consent under Regulation 2016/679.

[21] See Article 6(1) lit. e and c GDPR.

[22] See Article 6(1) lit. f GDPR. For external investigations, processing could be considered as "*necessary for the performance of a task carried out in the public interest*" pursuant to Article 6(1) lit. e GDPR. It is however unlikely that an internal investigation would, without more ado, qualify as a task carried out in the public interest, given that the basis for such interest must be laid down by EU or Member State law to which the investigator (as controller) is subject, cf. Article 6(3) GDPR. A unilaterally determined interest presented by a non-EU authority is therefore irrelevant. For private entities it is often not clear who makes the determination of what can be considered in the public interest. In both cases of either legitimate or public interest, the data subject has a right to object, cf. Article 21 GDPR.

and data protection). This balancing test is highly fact-based and must take into account such factors as the reasonable expectations of the individuals in relation to the privacy and security of their personal data, the nature and proportionality of the data processed, the principle of data minimization and purpose limitation as well as privacy-enhancing safeguards implemented by the parties involved (if any), all of which are discussed below.[23]

Data minimization

Personal data must be adequate, relevant and not excessive in relation to the purpose of the processing.[24] In short, this means that in the context of internal investigations or regulatory inquiries, companies may only process such types and amount of personal data as are strictly necessary to achieve the goals identified for the relevant internal investigation or governmental inquiry.[25] Note that data minimization also applies to any routine internal monitoring as well.[26] Under the GDPR, companies will also be required to carry out (and retain records of) an impact assessment for any data processing where the processing is "*likely to result in a high risk to the rights and freedoms of natural persons*".[27] Such impact assessments on a voluntary basis can also be a valuable tool to demonstrate safeguards put in place to protect the data and data subject's rights.

Purpose limitation

Personal data may only be collected and processed for specific, explicit and legitimate purposes, and may not be further processed in a way that is incompatible with those initial purposes.[28] It is therefore key to provide appropriate provisions in the company's internal policies relating to the collection and storage of personal data (e.g., the email and use of mobile phone policies) that expressly allow for onward processing of the collected data for purposes of conducting internal investigations and responding to governmental requests.

---

[23] Article 29 Working Party, WP 217, p. 34 and 42.

[24] Article 5(1)(c) GDPR.

[25] Finding the right balance depends on various factors, such as the seriousness of the possible offense being investigated, the evidence already available, the stage of the investigation, and the expected impact on the affected individuals.

[26] Article 29 Working Party, WP 249, Opinion No. 2/2017 on data processing at work, p. 23.

[27] Article 35 GDPR; see also Article 29 Working Party, WP 248 on Data Protection Impact Assessments and determining whether processing is "likely to result in a high risk" for the purposes of GDPR, which in the context of internal monitoring and internal investigations will have to be assessed on a case-by-case basis.

[28] Article 5(1)(b) GDPR; under GDPR, processing for a secondary purpose is permitted as long as it is compatible with the initial purpose of the data collection. Also, further processing for scientific research or statistical purposes is allowed.

Transparency and record keeping obligations

The GDPR increases transparency requirements, which has become an overarching data protection principle.[29] The data subject has the right to be notified of the processing of his or her personal data, the reason and legal basis for the processing, and whether data is to be transferred to a third country.[30] This can obviously create tension with the need for confidentiality in some circumstances.[31] Where the provision of information to a data subject would likely make it impossible to achieve the processing objectives, exemptions are available under certain circumstances.[32] In some cases, informing the data subject may even be prohibited, such as in connection with anti-money laundering ("AML") investigations, in which legislation makes it a criminal offence to inform an accountholder or a regulatory investigation.[33] In this situation, providing the data subject with information at the time of processing would obviously seriously impair the objectives of the legislation.[34]

Data controllers and processors are further under an express obligation under the GDPR to maintain adequate records of all processing activities, including in the context of internal investigations or regulatory inquiries.[35]

Rights of Data Subjects

As mentioned above, data subjects retain a number of rights under the GDPR, including rights of access and rectification, to object to processing.[36] Restrictions to these rights are permitted only under certain circumstances by EU law or at the

[29] Article 5 (1) a GDPR

[30] See Articles 12-14 GDPR. See also Article 29 Working Party, WP 260, Guidelines on transparency under Regulation 2016/679.

[31] There are some other limited exceptions to this information obligation, for example, if providing such information proves impossible or would involve a disproportionate effort, see Article 14(5) GDPR. See also Article 29 Working Party, WP 260, Guidelines on transparency under Regulation 2016/679.

[32] Article 14.5(b) and 23 GDPR. Exemptions may also be imposed by national Member State law, see recital 73 GDPR. One such example is Article 32 I of the French Data Protection Act 1978 which provides that data controllers are exempted from notifying data subjects when the "*processing of data is carried out for the purposes of preventing, investigating, identifying or prosecuting criminal offences*".

[33] See Article 39 of the 4th Anti-Money Laundering Directive (EU) 2015/849, implemented, for instance, in Sections 47 and 56(1) No. 60 of the German AML Act (*Geldwäschegesetz*), which provides for a fine up to EUR 5.000.000 under certain conditions. Article 55 § 1er and Article 81 § 6 of the respective Belgian *Loi du 18/09/2017 relative à la prévention du blanchiment de capitaux* [...] allows for administrative fines up to EUR 1.250.000 or 10% of the total annual net turnover, depending on the entity. Artt. 39, 55(4) of the respective Italian *Decreto legislativo 231/2007* as revised by *Decreto legislativo* 19/2017 allows the imposition of an up to one year's imprisonment or a fine up to EUR 30.000.

[34] See also Article 29 Working Party, WP 260, Guidelines on transparency under Regulation 2016/679, 28. General information should be provided however to all account-holders when an account is opened that their personal data may be processed for anti-money laundering purposes.

[35] Article 30 GDPR.

[36] Data subjects' rights are covered by Chapter III of the GDPR; A company can deny a data subject's objection if it demonstrates compelling legitimate grounds which override the interests of the data subject or if the processing is necessary for the establishment, exercise or defense of legal claims (Article 21(1) GDPR).

national member state law level, such as in the context of prevention, investigation or prosecution of criminal offences.[37]

PRACTICE TIP:
RESPONDING TO DATA SUBJECTS' REQUESTS

Companies must consider how early they will handle data subjects exercising their rights and the need to implement systems and controls in order to ensure that they can easily track and rectify personal data, extract it and/or provide it to individuals in the required format when the need arises.

Ensuring the Security of Collected Data

Companies undertaking an internal investigation or preparing a response to a governmental inquiry that involves the processing of personal data must implement appropriate technical and organizational measures to ensure the security of the personal data processed, including protection against unauthorized or unlawful processing and against accidental breach, disclosure or loss.[38] Guaranteeing general IT system security and integrity, as well as data encryption, are the most evident measures. Access to any internal compliance monitoring data should in particular be strictly limited within an organization on a need to know basis. In addition, access logs should be maintained and access rights must be reviewed on a regular basis.[39]

Data Retention

Personal data collected for compliance or investigative purposes must not be kept in a form that allows identification of the individuals to whom the data relates for any longer than strictly necessary for this purpose. If a company implements a monitoring policy, it will need to ensure that any personal data obtained as a result of the monitoring remains accurate and up to date[40] and is not retained longer than necessary to satisfy legitimate legal or business needs.

---

[37] Article 23 (1) d. GDPR

[38] Article 5(1) lit. f GDPR.

[39] See, for example, the European Data Protection Supervisor's Guidelines on processing personal information within a whistleblowing procedure (July 2016), pp. 10-11.

[40] See Article 5(1) lit. d GDPR.

Employee Data Protection

While the Directive did not include employment-specific provisions, Art. 88 of the GDPR now makes specific reference to data processing in the employment context. In particular, the EU data protection authorities have pointed out on several occasions that relying on employees' consent to legitimize processing of their personal data is problematic, as the imbalance of power between an employer and employee calls into question whether such consent could ever be given "freely".[41] Employers will therefore often have to look to another legal basis to justify processing of employee data in the context of internal investigations or when responding to governmental requests and take the rights of the employee into consideration.

PRACTICE TIP:
POLICY ON USE MONITORING OF IT EQUIPMENT

Companies must draft and make accessible to employees a policy concerning the purposes for which, when, and by whom, suspicious log data can be accessed and to guide them about acceptable and unacceptable use of IT work facilities. It is also considered best practice to evaluate this policy at least annually to assess whether the chosen monitoring solution delivers the intended results or whether there are other, less invasive tools or means available to achieve the same purposes.[42]

These rules also apply to monitoring of electronic communications in the workplace, and employers must consider the proportionality of the measures they are implementing, and whether actions can be taken to mitigate or reduce the scale and impact of the data processing.[43] The European Court of Human Rights (the "ECtHR") has recently re-affirmed[44] that employers should provide employees with a prior notice of monitoring clearly indicating:

[41] Article 29 Working Party, WP 249, Opinion No. 2/2017 on data processing at work, p. 6. The GDPR follows this approach and, in Recital 42, provides that "*consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment*", while recital 43 adds that, "*in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller*"; see also Article 29 Working Party, WP 259, Guidelines on Consent under Regulation 2016/679.

[42] Article 29 Working Party, WP 249, Opinion No. 2/2017 on data processing at work, p. 14. Article 29 Working Party, WP 249, Opinion No. 2/2017 on data processing at work, p. 14.

[43] Article 29 Working Party, WP 249, Opinion No. 2/2017 on data processing at work, p. 4.

[44] *Bărbulescu v Romania* (ECtHR, Grand Chamber, Application No. 61496/08, 5 September 2017).

— the possibility that employees' communications might be monitored;

— the nature and the extent of the monitoring measures implemented; and

the employers' legitimate reasons justifying the introduction of the monitoring measures.[45]

PRACTICE TIP:
A WELL-DRAFTED IT AND MOBILE-PHONE AND PERSONAL DEVICES POLICY

— Make sure you have clear, readily accessible and (where necessary) country-specific policies in place indicating, *inter alia*, the permitted uses of company devices and other IT equipment including messenger services; if you allow employees to use their own devices to perform work (so-called "*Bring You Own Device*", "BYOD"), make sure your policies adequately address the issues raised in that respect.

— Make sure you have informed (and are able to demonstrate that you have informed) employees before any monitoring activity takes place of the possibility of the monitoring, its nature and extent and the legitimate grounds justifying the implementation of monitoring measures.

— Assess whether it is necessary to carry out a data protection impact assessment (a "DPIA"), due to the characteristics of the technologies involved and the circumstances of the specific personal data processing at stake.

— Assess whether the adopted monitoring measures constitute the least intrusive means to achieve the stated purposes.

Finally, one other point bears mention (and requires care) – there is a carve-out provision in the GDPR regarding data protection in the employment context that leaves the door open to national implementing laws, which may result in country-by-country differences.[46] This problem is exacerbated by the fact that violations

[45] *Bărbulescu v Romania* (ECtHR, Grand Chamber, Application No. 61496/08, 5 September 2017). In the ECtHR's view, theoretical reasons, by themselves, do not constitute an actual risk for the employer, and would not support the adoption of monitoring measures.

[46] GDPR, Article 88: "*Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment*". Indeed, in several matters, the GDPR allows Member States to discretionally introduce legislative provisions aimed at completing requirements of the GDPR or at derogating to such requirements. In Germany, for example, processing of employee data may also be lawful due to collective bargaining agreements and internal collective agreements.

of employee privacy rights are often criminally sanctioned in EU member states, sometimes even in the absence of criminal intent.[47]

Whistleblowing Systems

Because a whistleblower system may be the source of information that leads to an investigation or even a company-wide crisis, companies should be aware of the data privacy implications involved to avoid sanctions from the national data protection authorities or damage claims of data subjects.[48] Data obtained through any whistleblowing system should always be processed with the greatest confidentiality and a high level of data security through adequate technical and organizational measures.[49]

In order to comply with the GDPR, companies should be sure to limit the scope of possible recipients of the whistleblowing reports, ensure the security of the information processed in the system and, to the extent that other data subjects' avail themselves of their right to access, apply a multi-step procedure to inform the relevant individuals concerned at the right time about how and why their data is being processed.[50] Limited storage periods should be set and all staff informed of their rights[51], as a premature disclosure may, in the individual case, impair the success of an internal investigation. Likewise, in order to avoid abuse of the whistleblowing system, its purpose must be clearly defined in written internal policies and procedures.[52]

---

[47] By way of example, employers in Italy conducting video surveillance in the absence of a prior agreement with the trade union representatives may be subject to a fine up to EUR 1.549 or face an up to one year's imprisonment, which may be imposed cumulatively in the event of a serious infringement pursuant to Article 38(1) and (2) of the Worker's Statute (*Legge n. 300/1970*, as modified by *Decreti legislativi n. 196/2003* and *n. 151/2015*).

[48] This applies especially to "false positives", which shall refer to any person being falsely accused by a "whistleblower" and struggling, despite presumed or even duly proven innocence, to continue its career.

[49] See Article 32 GDPR.

[50] For further detailed recommendations (applied to EU institutions, but equally useful for private enterprises), see also the European Data Protection Supervisor's Guidelines on processing personal information within a whistleblowing procedure (July 2016).

[51] See, for example, Art. 15 GDPR ("*Right of access by the data subject*") *et seq.*

[52] See European Data Protection Supervisor's Guidelines on processing personal information within a whistleblowing procedure (July 2016), pp. 5-6 (see *supra*, Fn. 70).

In addition, national EU member state law can lay down additional rules on whistleblowing[53] and enact more rigorous restrictions.[54] In France, for example, whistleblowing hotlines that fall outside the scope of the French Data Protection Authority (CNIL)'s so-called Single Authorization No. AU-004 on whistleblowing schemes[55], must request a specific authorization from CNIL to be able to lawfully implement the hotline.

USING EVIDENCE GATHERED IN VIOLATION OF PRIVACY LAWS: EXAMPLE GERMANY

Evidence gathered in violation of the GDPR or the Federal Data Protection Act (*Bundesdatenschutzgesetz*, "BDSG") can be inadmissible in German court proceedings, even though a general "fruit of the forbidden tree" doctrine is not recognized in German procedural law.[56] In a recent decision, the German Federal Labor Court (*Bundesarbeitsgericht*) held that obtaining personal data by means of a keylogger from an employee which lead to the employee's dismissal could not be used as evidence, as the requirements of the legal basis for obtaining the data under German data protection law were not met.[57]

Finally, whistleblowing systems must comply with local employment laws. For instance, in Germany and France consultation with a "works council" is mandatory prior to implementing a whistleblowing procedure. In addition, some jurisdictions do not allow the use of evidence obtained from anonymous whistleblowing in court proceedings (a stance that in some cases may conflict with EU privacy legislation

[53] The legal landscape of whistleblower protection in the EU is still heavily fragmented. Some countries, such as the UK (*Public Interest Disclosure Act*, 1998), Romania (*Legea nr. 571/2004 privind protecția personalului din autoritățile publice, instituțiile publice și din alte unități care semnalează încălcări ale legii*, 2004), Slovenia (*Zakon o integriteti in preprečevanju korupcije (ZIntPK)*, 2010), Serbia (*Zakon o zaštiti uzbunjivača*, 2015) and France (*Loi Sapin II*, 2016) have adopted such rules, whereas other countries, including Germany, still lack a comprehensive whistleblowing framework.

[54] For example, Section 171(1) of the UK Data Protection Bill (as currently drafted) introduces a criminal offence of recklessly or intentionally re-identifying an individual from anonymized data (without the consent of the data controller), which may hinder the ability to whistle-blow. There are certain exemptions to the prohibition where the re-identification is carried out in the reasonable belief that it is justified in the public interest (Section 171(4)(c)(iii)), or where it is proved necessary for the detection of crime (Section 171(6)(a)).

[55] The CNIL Single Authorization, amended most recently on June 22, 2017 through CNIL Decision No. 2017-191, sets out detailed data privacy requirements that must be complied with by companies implementing a whistleblowing system in France and generally covers systems that allow the reporting of, among others, criminal offences, manifest and serious infringements of international commitments of France, manifest and serious violation of laws, serious threats to the public interest, and behavior contrary to the company's code of conduct on corruption or drug trafficking. It does not cover, for example, facts or matters protected by medical secrecy, legal privilege and/or national security confidentiality.

[56] German Supreme Court decision of June 30, 2005, case no. BvR 1502/04 – in German

[57] Decision of July 27, 2017, case no. 2 AZR 681/16, cf. http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=en&nr=19516. – in German

requirements), and many jurisdictions do not allow an employer to contractually require an employee to "blow the whistle" and report on other employees.

Cross-border Transfers of Personal Data

In addition to the limitations described above with respect to processing data, additional restrictions apply to the transfer of personal data to countries outside of the European Economic Area ("EEA")[58] and specific safeguards need to be put in place. Companies should immediately begin considering these issues and familiarizing authorities and regulators outside of the EU with the issues raised by these limitations as soon as possible once an investigation begins.

Transfers within the EEA or to countries with an adequate level of protection

Cross-border transfers within the EEA are permitted provided they comply with the above-mentioned general requirements for processing personal data. Transfers of personal data outside the EEA may also be allowed where the European Commission has issued a so called adequacy decision finding that the third country provides an "adequate level of protection" (i.e., substantially equivalent to the level of protection offered in the EU).[59]

[58] As of the publication date of the present manual, the EEA consists of all 28 EU member states, plus Iceland, Norway and Liechtenstein. As regards the three latter states, the GDPR is currently under ongoing incorporation procedures into the EEA Agreement (see http://www.efta.int/eea-lex/32016R0679). Although Switzerland does not participate in this procedure, it is currently aligning its Data Protection Act to fulfill GDPR requirements.

[59] See Article 45 GDPR; http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm. As of the publication date of the present manual, the Commission has recognized Andorra, Argentina, Canada (only for commercial organizations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection.

UK: POST-BREXIT CROSS-BORDER TRANSFER

Brexit (i.e., the UK's contemplated withdrawal from the EU) is likely to take the UK outside of the EU data protection legislative framework with the following key implications:

— **Third country status** – on January 9, 2018, the European Commission issued a notice to stakeholders[60] confirming that the UK will become a "third country" for data protection purposes once the UK has left the EU. In the absence of an adequacy decision from the European Commission, the transfer of personal data from the EEA to the UK will therefore need to be made subject to Appropriate Safeguards or data exporters will need to rely on the one of the Specific Derogations.

— **UK Data Protection Bill** – the European Commission notice to stakeholders did not indicate whether the UK will be considered "adequate" following Brexit. However, the UK has already signaled that it intends for UK legislation substantially to mirror EU data protection laws going forward in order to minimize disruption. It has therefore introduced a new draft Data Protection Bill in September 2017 according to which the GDPR shall apply "*as if its Articles were part of an Act extending to*" the U.K., subject to some adjustments for the post-Brexit term.[61] This bill, should it be passed, might facilitate the process of obtaining an adequacy decision for the UK after Brexit.[62]

— **Timing** – the UK is scheduled officially to leave the EU on March 29, 2019.

Transfers to countries without an adequacy decision by the European Commission

As a general rule, transfers of personal data outside the EEA to countries not covered by a European Commission adequacy decision are prohibited[63] in order to "e*nsure that the high level of that protection continues where personal data is transferred to a [non-EU state]*".[64] Recital 115 of the GDPR expressly states that "transfers "*should*

[60] European Commission Notice to Stakeholders on the withdrawal of the United Kingdom from the Union and EU rules in the field of data protection (http://ec.europa.eu/newsroom/just/redirection.cfm?item_id=611943).

[61] Draft Data Protection Bill 2017 as of September 14, 2017 (https://www.gov.uk/government/collections/data-protection-bill-2017).

[62] Extra-territoriality provisions in the GDPR will in any event require UK organizations providing services or monitoring the behavior of persons within the EU to comply with their requirements, regardless of their im-plementation in UK law.

[63] Article 44 GDPR.

[64] Case C-362/14, Schrems v. Data Protection Commissioner, ¶ 72, ECLI:EU:C:2015:650.

only be allowed where the conditions of this Regulation for a transfer to third countries are met."

If a company needs to transfer data out of the EEA to a country without an adequacy decision in the context of an internal investigation or governmental inquiry, either a specific legal derogation must be relied on[65], or an appropriate alternative safeguard as outlined in the GDPR must be put in place.[66]

What are possible derogations or appropriate safeguards to transfer data to an affiliated group company outside the EEA?

Specific Derogations. The GDPR enumerates certain specific situations in which data can be transferred to third countries, even in the absence of an applicable European Commission adequacy decision.[67] Explicit consent by the data subject is an option again, but the same concerns raised before apply to consent in the context of transfer. In particular consent may be withdrawn at any time, making future processing (and transfer) illegal.

A derogation is available when the transfer would be "*necessary for the establishment, exercise or defense of legal claims*".[68] However, tThe scope of this derogation is unclear. Traditionally this derogation was interpreted in some member states to apply to judicial proceedings only (e.g., for discovery purposes in U.S. litigation),[69] but there is little authoritative guidance on the interpretation of this derogation under the new provisions of the GDPR or, more generally, on the scope of this derogation in the context of internal investigations, voluntary disclosures to regulators, and governmental inquiries.

---

[65] See Article 49 GDPR.

[66] See Article 46-47 GDPR.

[67] The GDPR adds transfers that are "*necessary for compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject*" (Article 49(1) 2nd sentence). It is unclear how this approach will work in practice given the lack of guidance on the suitable safeguards required and the need to inform the relevant supervisory authorities of transfers made pursuant to this derogation. While the European Commission stated in its Brief on behalf of the European Union as *Amicus Curiae* to the Supreme Court of the United States, United States v. Microsoft Corporation, 17-2, p. 15, that such interest could be recognized in "*not being subject to legal action in a non-EU state*", leading EU Data Protection And Privacy Scholars pointed out in their Brief as Amicus Curiae, p. 12, that "*a data controller's interest in complying with non-EU law is identical to an interest in not complying with the GDPR.*"

[68] See Article 49(1) lit. e GDPR. It is not clear yet how this interplays with the new Article 48 under the GDPR regarding judgments of foreign courts and decisions of administrative authorities (see below).

[69] Article 29 Working Party, WP 158, Working Document No. 1/2009 on pre-trial discovery for cross border civil litigation. Some member states such as Germany specified the claim requirements as "in court" in the national implementation of the Directive. These are no longer present in the harmonized GDPR text.

Appropriate safeguards. Another viable option to transfer data outside of the EEA, specifically in the context of internal investigations, is to put in place appropriate intra-group safeguards and ensure that enforceable protection of data subjects' rights and effective legal remedies are available. There are several ways to do this, including introducing binding corporate rules ("BCRs") at group level, having the relevant group entities enter into *ad hoc* contractual clauses based on the models adopted by the European Commission (or by a national data protection authority and approved by the Commission),[70] or adopting a specific data privacy tailored code of conduct,[71] or a certification mechanism[72] approved by the competent national data protection authority.

EU-U.S. Privacy Shield: adequacy based on self-certification. For companies based in the United States conducting an internal investigation or preparing a response to a governmental inquiry that also covers its European subsidiaries, the EU-U.S. Privacy Shield can offer a solution for *intra-group* data transfers or transfers to a data vendor. The Privacy Shield replaced the previously existing U.S. Safe Harbor scheme in July 2016, which was invalidated as a result of a legal challenge in EU courts.[73] Accordingly, U.S.-based companies may now elect to self-certify to the privacy principles set out in the Privacy Shield, and ensure compliance with those principles, in order to be authorized to transfer data from the EU to the US. While self-certification is relatively straightforward, monitoring compliance can be more difficult. The Privacy Shield passed its first review at the EU level, but legal challenges are pending.[74]

What are grounds to transfer data to governmental authorities outside the EEA?

The same means to transfer data that apply in an intra-group context would, in theory, also be available for (onward) transfers to a public authority. In practice,

[70] Where contractual clauses were authorized under the Directive as providing appropriate safeguards for the transfer of personal data to a third country, the GDPR provides that these authorizations will remain valid until amended, replaced or repealed (Article 46(5) GPDR).

[71] Based on the new scheme in Article 40 GDPR.

[72] Based on the new scheme in Article 42 GDPR.

[73] See also Article 29 Working Party, WP 238, Opinion No. 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision.

[74] The European justice commissioner and the Article 29 Working Party have also expressed the need for improvement of the Privacy Shield in some areas, in default whereof members of the latter announced bringing the Privacy Shield Adequacy decision to national courts to pave the way for a preliminary ruling of the CJEU. See, Article 29 Working Party, WP 255 on First annual Joint Review of the EU—U.S. Privacy Shield..

however, there are a number of additional complications that arise when personal data collected and processed within a corporate group is disclosed and transmitted outside of the group to public authorities. Adequate privacy-enhancing safeguards must be considered before transferring any personal data across borders to a court or other governmental authority, such as requesting a protective order in a litigation context (shielding the personal data from public disclosure)[75] or redacting documents for personal data (especially sensitive data) prior to any transfer.

Transfer to courts or administrative authorities. Article 48 of the GDPR, which specifically addresses disclosures ordered by non-EU states, provides that "*any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the third country and the Union or a Member State* [...]".[76] Article 48 of the GDPR expressly states that a request, for instance from a court in a third country, does not make a transfer legal, and indicates otherwise that mutual legal assistance treaties (MLATs) are the preferred transfer option given their "*carefully negotiated balance between the interests of different states* [...] *designed to mitigate jurisdictional conflicts*".[77] Of course, one issue with this approach is that it limits the ability to transfer data to those instances where such agreements have already been executed.[78] Further guidance from the data protection authorities and ultimately the Court of Justice of the European Union may be needed.

---

[75] Article 29 Working Party, WP 158, Working Document No. 1/2009 on pre-trial discovery for cross border civil litigation, p. 11.

[76] See Article 48 GDPR. See also recital 115 GDPR.

[77] See Brief of the European Commission on behalf of the European Union as *Amicus Curiae* to the Supreme Court of the United States, United States v. Microsoft Corporation, 17-2, p. 14. The Article 29 Working Party recently underlined in a statement on e-evidence of November 29, 2017 that MLATs "*must—as a general rule—be obeyed when law enforcement authorities in third countries request access or disclosure from EU data controllers. The circumvention of existing MLATs* [...] *is therefore an interference with the territorial sovereignty of an EU member state*." See also Brief of Jan Philipp Albrecht *et al.*, Members Of The European Parliament as *Amicus Curiae* to the Supreme Court of the United States, United States v. Microsoft Corporation, 17-2, pp. 18 *et seq.*, referring to European Parliament resolutions expressing concern over the circumvention of MLATs.

[78] See, for example, the MLAT in criminal matters between Germany and the US signed on October 14, 2003, whose bilingual version can be found in the Federal German Law Gazette, see http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl207s1618.pdf. In a written statement of January 31, 2007, Germany's Federal Ministry of Justice expressed its legal opinion on the precedence of this MLAT, see https://datenschutz-berlin.de/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2007-Web.pdf, pp. 186 *et seq.* Thus, seizure orders from US authorities directly addressed to private bodies in Germany are considered contrary to the Germany-US MLAT. Rather, pursuant to Article 1(5) *loc. cit.*, the German data protection authorities held the opinion that US authorities were at first required to "*request assistance pursuant to the provisions of this Treaty to obtain* [...] *documents, records, and other items*" in the German territory. Given the wording of Article 48 GDPR that applies "*without prejudice to other grounds for transfer pursuant to this Chapter*", it remains to be seen whether a voluntary transfer may also be permitted by virtue of Article 49 GDPR, irrespective of any official request for mutual legal assistance. The key issue remains a potential circumvention of existing MLATs (*see supra*, Fn. 101).

Finally, note that Article 48 applies "*without prejudice to other grounds for transfer pursuant to this Chapter*", so that the specific derogations afforded under Article 49 of the GDPR (described above) would still apply.[79]

Standard Contractual Clauses and internal safeguards not available. Companies will not be able to use the abovementioned Standard Contractual Clauses for transferring data to authorities, as the authorities will generally be unwilling or unable to enter into a binding contractual relationship with the company.[80] The group-internal specific safeguards, such as BCRs and codes of conduct, will likewise not be available in that situation.

"EU" public interest derogation. Apart from derogation for the establishment, exercise or defense of legal claims described above, which is primarily intended for use in the context of civil proceedings, the GDPR also provides a derogation for transfers necessary for important reasons of public interest[81], which more naturally applies in the context of law enforcement. It may be wise to assume that this derogation may be construed narrowly by European data privacy authorities and courts, such that only the interests identified as such by national legislation applicable to data controllers established in the EU will satisfy this "public interest" requirement (i.e., defined by EU or members state law under the supervisory jurisdiction of the CJEU).[82]

[79] See Brief of the European Commission on behalf of the European Union as *Amicus Curiae* to the Supreme Court of the United States, United States v. Microsoft Corporation, 17-2, p. 15.

[80] The Standard Contractual Clauses approved by the European Commission would for example claim to subject government agencies to the jurisdiction of EU data protection authorities and in the U.S. for example in many situations government authorities are prohibited from disclosing or granting further protection to certain personal information. See also David C. Shonka, *Cross Border Transfers—Producing Information from the EU to U.S. Government Agencies*, 17 DDEE 658 (2017).

[81] Recital 112 and Article 49(1) lit. d GDPR. See also Brief of the European Commission on behalf of the European Union as *Amicus Curiae* to the Supreme Court of the United States, United States v. Microsoft Corporation, 17-2, p. 15, referring to Article 83 TFEU stating particularly serious areas of crime.

[82] See Article 29 Working Party, WP 114, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, p. 15; this interpretation prevents circumvention by foreign authorities of the requirement for adequate protection and is currently supported by leading EU Data Protection And Privacy Scholars in their Brief as *Amicus Curiae*, United States v. Microsoft Corporation, 17-2, p. 11.

PRACTICE TIP:
SEDONA PRINCIPLES

The Sedona Conference (a nonprofit research and educational institute) regularly publishes guidelines and principles for addressing data protection in cross-border investigations, including in the context of government & internal investigations and on discovery, disclosure and data protection.[83] These principles are a useful resource for companies confronted with the issues described in this chapter.

Other Legal Restrictions

Other obstacles to data processing in the context of investigations can arise to varying degrees on a member state level.

France

In France, a Blocking Statute limits foreign discovery on French soil. Act 80-538 prohibits the communication of economic, commercial, industrial, financial or technical information to serve as proof in foreign administrative or judicial proceedings and imposes criminal sanctions for doing so. The prohibition covers French nationals, residents and officers, representatives, agents or employees of an entity with a head office or establishment in France. Such information may be communicated under limited circumstances, such as where the communication is permitted under French Law or an international treaty or agreement, such as the Hague Convention.[84]

In its guidance regarding data transfers for pre-trial discovery from July 2009, the French Data Protection agency CNIL expressly considers data transfers not in compliance with the Hague Convention "unlawful" under French data protection law.[85]

[83] See the Sedona Conference International Principles for Addressing Data Protection in Cross-Border Gov-ernment & Internal Investigations: Principles, Commentary & Best Practices, May 2017; the Sedona Con-ference International Principles on Discovery, Disclosure & Data Protection – Jan 2017 Transitional Edition, January 2017.

[84] Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555, T.I.A.S. No. 7444, 847 U.N.T.S. 231.

[85] CNIL, Deliberation No. 2009-474 of 23 July 2009, concerning recommendations for the transfer of personal data in the context of U.S. court proceedings known as "Discovery."

Germany

In Germany[86], the Telemedia Act (*Telemediengesetz*, "TMG") and the Telecommunications Act (*Telekommunikationsgesetz*, "TKG"), both implement the ePrivacy Directive 2002/58/EC and seek, inter alia, (1) to protect the secrecy of telecommunications, safeguarded in Article 10 of the German Constitution, and (2) impose significant restrictions on the use of information sent through electronic communication. This may create additional obstacles for companies trying to obtain information stored on electronic devices used by personnel, in particular in the case of internal investigations of employees' private devices (BYOD). It is therefore important to set up a comprehensive corporate agreement on the business use of private equipment, and vice versa. Such a company agreement should grant control and access rights and state as accurately as possible whether screenings are done regularly or only in the event of doubt, and involve the co-determination of the works council. Failure to comply may result in administrative fines or criminal sanctions, such as an up to five years' imprisonment or a fine. Moreover, evidence gained from such violations may be considered inadmissible in court proceedings.

Other EU jurisdictions have similar restrictions in place in their respective ePrivacy Directive implementing measures, often also backed up by criminal sanctions.[87] In addition, obstacles to investigations and subsequent transfers may also arise from other areas such as labor law, professional or banking secrecy restrictions.

[86] See, *AccessData Corp. v. Alste Tech. GmbH*, 2010 WL 318477, Court for the District of Utah on January 21, 2010. The Court held that "*even assuming that* [Section 4c of the German Data Protection Act] *prohibited disclosure of personal third-party information, the United States Supreme Court has held* [in the Aerospatiale decision] *that '[i]t is well settled that such* [blocking] *statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute'*."

[87] See, for example, Article 145 of the Belgian Act on Electronic Communication of June 13, 2005.

PRACTICE TIP:
IDENTIFY RELEVANT JURISDICTIONS AND ENGAGE LOCAL COUNSEL EARLY

Companies should identify relevant jurisdictions and engage local counsel in those jurisdictions from the onset of any internal investigation or external investigation process that is subject to European data privacy laws. It is critical to understand where data is collected, where the individuals whose data is processed are located and which national laws apply.[88]

Swiss Data Privacy Rules and Blocking Statute

Federal Act on Data Protection

Swiss data protection laws are currently still governed by the Federal Act on Data Protection ("DPA") of June 19, 1992 (as amended), and the Federal Ordinance on Data Protection of June 14, 1993. Additionally, as in member states of the EU, data protection rules can be found throughout the legislative body of Switzerland, most notably the Swiss Federal Code of Obligations, which governs the processing of employee data in particular. A draft bill intended to adapt the Swiss federal Data Protection Act to reflect changes interlocked in the EU by the GDPR[89] as well as the amendments to Convention 108 has been proposed in September 2017.[90] That said, Swiss law employs concepts of personal data controller, processor, data subject and processing that are all similar to the GDPR. Failure to comply with the DPA provisions may lead to criminal sanctions and fines of up to CHF 250,000.

[88] See also Principle 1, Comment 1b of Sedona Conference International Principles for Addressing Data Pro-tection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices, May 2017, p. 20; see also Cleary Gottlieb, "Selected Issues for Boards of Directors in 2018, 22, https://www.clearygottlieb.com/-/media/files/boards-of-directors-2018/selected-issues-for-boards-of-directors-2018-final-x2.pdf.

[89] The revised Swiss DPA further aims to pursue the goals of the (future) Police and Criminal Justice Authorities Directive 2016/680 because of the Schengen Agreement. The revised DPA will bring about amendments to other laws, inter alia to the Swiss Federal Penal Code and the Codes on Penal and Civil Procedure. For instance, the latter provides that court fees will not apply to court proceedings that concern the revised DPA.

[90] A preliminary draft has been issued on December 21, 2016.

PRACTICE TIP

The Swiss DPA is not applicable to data in international mutual legal assistance proceedings.

In the employment context, the employer owes employees specific care in Switzerland under the Code of Obligations in addition to the DPA, with regard to protecting the employee's rights. This restricts an employer's access to an employee's professional data.

Restrictions to data transfers out of Switzerland are similar to those in the EU. Certain countries are identified as providing adequate protection (EEA countries for instance), and there are safeguards that can be applied similar to in the EU (such as binding corporate rules, the Privacy Shield, and data transfer agreements). Article 6 of the current DPA[91] lists derogations that may apply outside of that, such as "*establishment, exercise, or enforcement of legal claims before the courts*" (Article 6, 2nd sentence, (d)[92]).

Blocking Statutes

In Switzerland two articles in « Crimes and Misdemeanors against the State and Defense » of the penal code protecting Swiss sovereignty and Swiss trade or business secrets against foreign requests can be pertinent to investigations.

First, Article 271 prohibits a foreign country from undertaking acts in Swiss territory that are in the competence of Swiss authorities, which includes the gathering of evidence for use in foreign proceedings (criminal, civil, or administrative). This may extend to remote access to such data as well. Data may only be collected through channels of judicial assistance such as the Hague Convention or MLATs.

Second, Article 273 prohibits disclosing third-party business secrets to foreign states and entities, without their consent. Third parties are include customers and business

[91] Article 13 of the latest draft bill.

[92] Article 14, 1st sentence, lit. c, (2) of the latest draft bill.

partners. The protected information must have a sufficient nexus to Switzerland to trigger Article 273. Disclosure through legal assistance proceedings is again possible. Violation of either Article carries a prison sentence or fine.

Key Steps to Prepare

— Companies should develop protocols addressing the production and transfer of information to authorities within reasonable timeframes. Companies should have a response team with data privacy experience that is prepared to deal with data processing and production questions on short notice.[93]

— When an authority is already involved in the investigation, companies should engage in a dialogue at an early stage regarding the gathering and transferring of data in order to make sure it is aware of EU data protection laws to communicate potential obstacles and potential delays.[94]

— Local counsel should be consulted early on to ensure compliance with local laws.

[93] See Principle 1 of the Sedona Conference International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices, May 2017, p.19.

[94] See Principle 4 of the Sedona Conference International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices, May 2017, p.24.