Skadden

Privacy & Cybersecurity Update

European Commission Publishes Draft Adequacy Decision on EU-US Data Privacy Framework

The European Commission (EC) has published a draft adequacy decision on the EU-U.S. Data Privacy Framework in an effort to reestablish a legal regime for the transfer of personal data from the EU to the U.S.

On December 13, 2022, the EC published a draft decision on the adequate level of protection of personal data under the EU-U.S. Data Privacy Framework.[1] The draft decision comes approximately two months after President Joe Biden signed an executive order on "Enhancing Safeguards for the United States Signals Intelligence Activities," which established new regulations for the collection and use of personal data by U.S. intelligence agencies.[2] The executive order and adequacy decision are intended to implement a new EU-U.S. framework to allow for the free flow of personal data from the EU to the U.S. under EU law after the 2020 *Schrems II* decision that invalidated the Privacy Shield, the prior privacy framework between the two jurisdictions.[3]

The draft decision will now be examined by other EU institutions before the EC adopts a final adequacy decision, which can be expected by mid-2023.

Background

In *Schrems II*, the Court of Justice of the European Union (CJEU) invalidated the EU's Privacy Shield decision (Decision 2016/1250 on the adequacy of the protection provided by the Privacy Shield), citing concerns over U.S. public authorities' access to and use of EU personal data, and the lack of an adequate redress mechanism that EU data subjects could use against such public authorities. As a result of the decision, transfers of personal data from the EU to the U.S. on the basis of the Privacy Shield framework became illegal immediately. Companies were therefore obliged to implement a valid data transfer mechanism (*e.g.*, the EC's Standard Contractual Clauses (SCCs)) for the transfer of personal data from the EU to the U.S. and to conduct a transfer impact assessment (TIA) for each transfer. This decision equally applied to the transfer of personal data from the U.K. to the U.S., as the CJEU decision was made during the Brexit transition period and the U.K. GDPR (the U.K. counterpart to the EU GDPR) is materially aligned with the EU GDPR.

[1] The draft decision is available here.

[2] The executive order can be accessed here.

[3] Skadden's analysis of *Schrems II* is available here.

Transfer of Personal Data Outside the EU

Under the EU GDPR, personal data may not be transferred outside the EU unless (1) an appropriate safeguard is put in place (*e.g.*, the SCCs), (2) the transfer is to a country covered by an EC adequacy decision,[4] or, (3) as a last resort, an exemption applies (*e.g.*, an individual whose personal data is transferred explicitly consents to the transfer). Where the EC adopts an adequacy decision in favor of a destination country, personal data can flow freely from the EU to such country without the need to put in place any additional arrangements (*e.g.*, the SCCs). These rules equally apply to the transfer of personal data outside the U.K., although the U.K. government (not the EC) is responsible for issuing adequacy regulations under the U.K. GDPR following Brexit.

Reasons for Draft Adequacy Decision

In its draft decision, the EC has concluded that the U.S. does ensure an adequate level of protection for the transfer of personal data from the EU to the U.S., noting that President Biden's recent executive order provides enhanced safeguards.[5] In particular, the EC highlighted that the executive order establishes (1) binding safeguards that limit access by U.S. intelligence services only to data that is necessary and proportionate to protect U.S. national security, (2) enhanced oversight of U.S. intelligence services to ensure compliance with the executive order, and (3) an independent and impartial two-tier redress mechanism to investigate and resolve complaints from EU data subjects about U.S. intelligence services access to their personal data.

Two-tier Redress Mechanism

The EC noted that the new two-tier redress mechanism is a "significant" improvement compared to the Privacy Shield's U.S. data ombudsman mechanism, which was criticized for its lack of independence, investigative powers and binding authority.

Under the first tier of the redress mechanism, individuals — through the appropriate public authority from a "qualifying state" — will be able to file a complaint with the civil liberties protection officer (CLPO). Accordingly, as the EU is intended to be a "qualifying state," EU data subjects will be able to utilize this new two-tier redress mechanism. Within 15 business days of receipt of the complaint, the CLPO will conduct an initial review to determine whether the complaint is a "qualifying complaint" (*e.g.*, occurred after October 7, 2022, involves personal data from a "qualifying state" and adversely affect the complainant's privacy and civil liberties). Based on the results of this investigation, the CLPO will determine whether a violation of the executive order has occurred.

If dissatisfied with the outcome, under the second tier of the redress mechanism the complainant will be able appeal the decision by the CLPO to the Data Protection Review Court (DPRC), which will be composed of a three-panel judge panel. These judges must not be members of the U.S. government, must have relevant experience in data privacy and national security law, and must be protected against removal (except where there is a serious cause for dismissal such as a conviction of a criminal offense). In addition, the DPRC must appoint a "special advocate" to represent the complainant at the court. However, while DPRC judges are supposed to provide "independent and impartial review[s] of applications," the regulations note that the U.S. attorney general is responsible for appointing judges to the DPRC (although such judges will not work under the supervision of the attorney general) and that the DPRC will be established within the Department of Justice. Though similar to the status of a special counsel (who operates independently but is appointed and can be dismissed by the attorney general), the level of involvement of the attorney general and the Department of Justice has led some to express skepticism as to whether the DPRC will be truly independent.

Next Steps

The decision will now be reviewed by the European Data Protection Board (EDPB), which will issue a nonbinding opinion. The European Parliament can also adopt a nonbinding position, but has no formal role in the adoption process. The EC will then request approval of the decision by the Council of the European Union (Council), which is made up of government ministers from each EU Member State. In order to be approved by the Council, the decision must receive a qualified majority of approval from 55% of EU Member States (15 out of 27) representing at least 65% of the total EU population. If at least four Council members vote against the decision, the decision will not be approved. Once approved by the Council, the EC will formally adopt the decision, which will be published in the EU Official Journal and take immediate effect.

The approval process typically takes several months; for the Privacy Shield, the process took five months whereas the process was completed in four months for the U.K. adequacy decision. European Commissioner Justice Didier Reynders has said that he expects the final decision in this instance to be adopted by July 2023.

Separately, the U.K. government has said previously that it is working "expeditiously" to review the enhanced safeguards and redress mechanism in the executive order as part of its

[4] The EC has published adequacy decisions in favor of the following countries and territories: Andorra, Argentina, Canada (commercial organizations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the U.K. and Uruguay.

[5] Skadden's analysis of the executive order is available here.

assessment of U.S. data protection laws and practices. The U.K. government has said that it intends to present adequacy regulations in Parliament in early 2023 to restore the free flow of personal data between the two jurisdictions. Meanwhile, the U.S. government has said that it intends to designate the U.K. as a "qualifying state" under the executive order, which would mean U.K. data subjects also could utilize the enhanced privacy and civil liberties outlined in the executive order (*e.g.*, the two-tier redress mechanism).

Max Schrems, who brought the *Schrems II* case before the CJEU, has criticized both the executive order and the EC's draft decision. In particular, Mr. Schrems has criticized the independence of the DPRC, which, according to him, will not be a court within the legal meaning of Article 47 of the EU's Charter of Fundamental Rights or the U.S. Constitution. Additionally, Mr. Schrems has said that the U.S. and EU interpretations of the words "necessary" and "proportionate" are not aligned, meaning U.S. intelligence surveillance activities will fall short of the standard required under EU law. Mr. Schrems also has warned that the EC's final decision may be open to fresh legal challenges, as it "will likely not satisfy the CJEU."

Key Takeaways

The draft decision is welcome news for companies that transfer personal data from the EU to the U.S. While such transfers of personal data are not currently illegal, they are more cumbersome to implement than previously under the Privacy Shield framework. If the decision is adopted, organizations will need to be certified, which will require them to commit to comply with a detailed set of privacy obligations (*e.g.*, purpose limitation, data retention). However, the adoption of an adequacy decision by the EC is not guaranteed, and any such decision may be subject to fresh legal challenges.

In the meantime, it remains business as usual for companies that transfer personal data from the EU to the U.S. or from the U.K. to the U.S., meaning companies must continue to rely on a valid data transfer mechanism and conduct a TIA for each transfer of European or U.K. personal data to the U.S.

Return to Table of Contents

UK Information Commissioner's Office Publishes Guidance on International Transfers and Transfer Risk Assessments

The U.K.'s supervisory authority for data protection, the Information Commissioner's Office (ICO), published new guidance on internal transfers of personal data outside the U.K. and transfer risk assessments (TRAs) as well as a new template for organizations conducting TRAs.

On November 17, 2022, the ICO published updated guidance on "International Transfers"[6] and "Transfer Risk Assessments (TRAs),"[7] which provide welcome clarity on the rules governing international transfers of personal outside the U.K. under the U.K. GDPR. Additionally, the ICO published its "TRA tool,"[8] which offers an alternative method for completing TRAs to the approach recommended by the EDPB for transferring personal data outside the EEA under the EU GDPR.[9]

Overview of the Rules Governing Restricted Transfers

Since the end of the transition period on December 31, 2020, the U.K. GDPR has governed restricted transfers, which are transfers of personal data outside the U.K. to third countries. Unless a restricted transfer is to a country covered by U.K. adequacy regulations[10] or subject to one of the exceptions (see "Exceptions to the Rules on Restricted Transfers" below), the organization making the restricted transfer must put in place "appropriate safeguards." These safeguards are listed in Article 46 of the U.K. GDPR and include entering into the International Data Transfer Agreement (U.K. IDTA), the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (U.K. Addendum), or, for intra-group data transfers, the Binding Corporate Rules (BCRs).

Examples of Restricted Transfers

The ICO guidance categorizes restricted transfers into three broad circumstances, discussed below.

1. The UK GDPR Applies to the Personal Data Being Transferred

The ICO guidance offers the example of an Australian retailer that collects personal data of U.K. customers via its website.[11] While the U.K. GDPR would apply to the processing of such personal data by the Australian retailer (as the customers are located in the U.K.), the transfer of personal data initiated and agreed to by the U.K. customers on the Australian retailer's website would not be a restricted transfer.

[6] See the ICO's International Transfer guidance.

[7] See the ICO's Transfer Risk Assessments guidance.

[8] See the ICO's TRA tool.

[9] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

[10] The U.K. has adequacy regulations with the following countries and territories: the European Economic Area member states, the European Free Trade Association states (*i.e.*, Iceland, Liechtenstein, Norway and Switzerland), Gibraltar, Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, South Korea (as of December 19, 2022), Japan (for private sector organizations only) and Canada (for data subject to Canada's Personal Information Protection and Electronic Documents Act only).

[11] We have adapted examples from the ICO guidance throughout this article for clarity.

However, if the Australian retailer used an Australian website management company to run its website, any transfer of the U.K. customers' personal data from the Australian retailer (and initiated and agreed to by the Australian retailer and not the U.K. customer) to the Australian website management company would constitute a restricted transfer.

2. The Organization Initiates and Agrees to the Transfer or Makes the Personal Data Available to an Organization Outside the UK

Where the sending party (a controller or processor) enters into an agreement with the receiving party for the transfer of data outside the U.K., the sending party will be deemed to have initiated and agreed to the restricted transfer.

The ICO guidance contains numerous examples of what is meant by "initiates and agrees to" regarding the transfer, including the following:

i. If (1) a U.K. health care company (the U.K. controller) enters into an agreement with a U.K. data analytics company (the U.K. processor) for the processing of patient data, and (2) the U.K. data analytics company enters into a separate agreement with a U.S. data analytics company (the U.S. sub-processor) to conduct such processing, the restricted transfer would occur between the U.K. processor and the U.S. sub-processor. This is because the U.K. processor will have initiated and agreed to send the data to the U.K. sub-processor in a sub-processor agreement containing the relevant processor-to-processor (P2P) details in the U.K. IDTA or P2P module in the U.K. Addendum. This would still be the case even if the personal data was transferred directly from the U.K. controller to the U.S. sub-processor as the U.K. processor (not the U.K. controller) initiated and agreed to the transfer in the sub-processor agreement. This is without prejudice to the fact that the U.K. processor must have obtained general or specific authorization from the U.K. controller to appoint the US sub-processor, as required under Article 28 of the EU GDPR/U.K. GDPR. However, if the U.K. controller instructed the U.K. processor to transfer the personal data to the U.S. sub-processor, then the restricted transfer would occur between the U.K. controller and the U.S. sub-processor (even if the personal data flowed from the U.K. processor to the U.S. sub-processor) as, in this instance, the U.K. controller (not the U.K. processor) initiated and agreed to the transfer and the U.K. processor is acting on the U.K. controller's instructions.

ii. If a U.K. company (the U.K. controller) has separate contracts with a HR data analytics company in the U.K. and Mexico (the U.K. and Mexico processors, respectively), any transfers of personal data from the U.K. processor to the Mexico processor at the request of the U.K. controller would be a restricted transfer between the U.K. controller and the Mexico processor (even if the personal data flows directly from the U.K. processor to the Mexico processor). This is because the U.K. controller initiated and agreed to the transfer.

The ICO guidance also makes it clear that providing *access* to personal data to an organization outside the U.K. constitutes a restricted transfer (even if the personal data remains in the U.K.). For example, if a U.K. company grants access to its IT systems (which are hosted on a U.K. server) to an Indian IT support company, this would be a restricted transfer. By contrast, if personal data merely transits through another country, but is never accessed in such country, this would not be a restricted transfer.

3. The Receiving Organization is a Separate Controller or Processor, and is Legally Distinct From the Sending Organization

This could be a separate sole trader, partnership, limited company, public authority or other legal entity. The ICO guidance emphasizes the fact that restricted transfers may occur between two organizations in the same group (*e.g.*, a U.K. company that transfers employee data to its parent company in the U.S. as part of the group's centralized HR system).

Responsibility for Complying With the Rules on Restricted Transfers

Only the organization that initiates and agrees to the restricted transfer is responsible for complying with the rules on such transfer. This could be the controller or processor of such data. However, even where a controller or processor is not required to comply with the rules on restricted transfers, they may have other obligations under the U.K. GDPR. In the example under point (1) above, the U.K. health care company (the U.K. controller) would still be required to conduct due diligence on the U.K. data analytics company (the U.K. processor) to ensure it complies with the rules on restricted transfers.

Conducting a TRA

As confirmed by the CJEU in *Schrems II*,[12] whenever an organization is relying on an appropriate safeguard (*e.g.*, U.K. IDTA, U.K. Addendum), it must conduct a TRA. This applies to transfers of personal data outside the U.K. or the EEA.

According to the ICO guidance, TRAs should address the risks to people's rights arising from:

i. third parties in the destination country (that are not bound by the appropriate safeguard) accessing the personal data (in particular, government and public bodies); and

ii. difficulties arising in enforcing the appropriate safeguard.

The ICO guidance provides clarity on who is responsible for conducting a TRA. In particular, the ICO guidance notes that:

- If a processor is making the restricted transfer on behalf of the controller, only the processor must complete the TRA. However, the controller must carry out reasonable and proportionate checks to ensure that any restricted transfers the processor makes on behalf of the controller are compliant with the U.K. GDPR (including in respect of a TRA).
- If the receiver of the personal data further transfers the personal data to third parties, such as by making an onward transfer: (1) the sender must carry out a TRA for this onward transfer, *or* (2) the receiver must carry out a TRA and provide the sender with evidence that it has done so in compliance with the requirements of the relevant data transfer mechanism.

ICO Approach vs. EDPB Approach

As noted above, the ICO's new TRA tool offers an alternative, risk-based approach to conducting TRAs. The key difference between the approach of the ICO and the EDPB is the emphasis of the assessment as set out in the comparison table below:

- The ICO approach compares the position of the individuals whose personal data is transferred if (1) the personal data remains in the U.K., and (2) the personal data is transferred outside the U.K.
- The EDPB approach compares more generally the laws and practices of the exporting country (sender) with those of the importing country (receiver).

[12] Skadden's analysis of *Schrems II* is available here.

TRA Comparison Table

ICO Approach	EDPB Approach
Question 1: What are the specific circumstances of the restricted transfer?	**Step 1:** Know your transfers.
Question 2: What is the level of risk to people in the personal information you are transferring?	**Step 2:** Identify the transfer tools you are relying on.
Question 3: What is a reasonable and proportionate level of investigation given the risk level in the personal information and the nature of your organization?	**Step 3:** Assess whether the Article 46 of the EU GDPR transfer tool being relied on is effective in light of all circumstances of the transfer.
Question 4: Is the transfer significantly increasing the risk for people of a human rights breach in the destination country?	**Step 4:** Adopt supplementary measures.
Question 5: a. Are you satisfied that both you and the people the information is about will be able to enforce the Article 46 transfer mechanism against the importer in the U.K.? b. If enforcement action outside the U.K. is needed, are you satisfied that you and the people the information is about will be able to enforce the Article 46 transfer mechanism in the destination country (or elsewhere)?	**Step 5:** Procedural steps if you have identified effective supplementary measures.
Question 6: Do any of the exceptions to the restricted transfer rules apply to the significant risk data you have identified?	**Step 6:** Reevaluate at appropriate intervals.

Additionally, the ICO TRA tool provides organizations with a pragmatic, user-friendly template containing a series of six broad questions (with step-by-step guidance, tables and sub-questions for each of these broad questions). By contrast, the EDPB does not offer organizations a template TRA. Instead, it provides comprehensive guidance on the six steps that organizations should follow when conducting a TRA (see "TRA Comparison Table" above).

A significant divergence in the ICO approach is the introduction of "low harm risk" transfers. Where an organization concludes that all the categories of personal data being transferred are "low harm risk" (see Question 2 in "TRA Comparison Table" above), it may proceed with the restricted transfer without completing the rest of the TRA. This approach represents a divergence from the EDPB approach, which requires an assessment of local laws in all circumstances. To determine whether a transfer is "low harm risk," an organization must first assign an initial risk score to each category of personal data being transferred and then consider aggravating factors (*e.g.*, confidentiality, large volume, information about children) and mitigating factors (*e.g.*, information in the public domain). The Appendix to the TRA tool contains a list of indicative initial risk scores for various categories of personal data. For instance, name, age, contact details and date of birth are examples of "low" risk data, whereas race, medical records, location data and sexual orientation are examples of "high" risk data. While such indicative risk scores are helpful, there is danger in that such scores are overly simplistic (with no clarity provided in the ICO guidance on the rationale for the indicative risk scores, or how to increase or decrease the final risk score based on the aggravating and mitigating factors identified).

The ICO notes that it is happy for organizations to conduct TRAs in line with either the ICO or EDPB approach; however, the ICO approach is unlikely to be beneficial to organizations that transfer personal data outside the U.K. *and* the EEA and that are eager to standardize their approach to such transfers (as these organizations must continue to comply with the EDPB approach for any transfers of personal data outside the EEA). As such, the TRA tool is more likely to be helpful to organizations that only transfer personal data outside the U.K.

Exceptions to the Rules on Restricted Transfers

There are eight specific derogations under Article 49 of the U.K. GDPR to the requirement to put in place appropriate safeguards for restricted transfers. Where a derogation applies or there is a transfer to a country covered by U.K. adequacy regulations, an organization is not required to conduct a TRA.

Necessary and Proportionate

It must be both "necessary" and "proportionate" to rely on the derogations (with the exception of explicit consent), otherwise, an organization must either obtain explicit consent (see "Explicit Consent From the Individual" below) or put in place an appropriate safeguard (*e.g.*, U.K. IDTA, U.K. Addendum).

The ICO guidance notes that "necessary" means more than "useful and standard practice," but not "absolutely essential."

In terms of proportionality, the ICO guidance contains a list of factors that organizations should consider when determining whether a data transfer mechanism (*e.g.*, U.K. IDTA, U.K. Addendum) or a derogation is more proportionate. For example, it is more likely to be proportionate to rely on a derogation where (1) there is an occasional transfer, (2) the volume of data transferred is low, (3) there is a low risk of harm to individuals once their personal data is transferred, and (4) there are other protections available for the personal data (though none are specified in the ICO guidance).

Examples of Derogations

The ICO guidance contains a helpful walk-through of the eight derogations illustrated with examples. We examine some of the key derogations below.

1. **Explicit Consent From the Individual**

   An organization can make a restricted transfer if it obtains specific and informed consent from the individual whose personal data would be the subject of the restricted transfer. To ensure that such consent is valid, the ICO recommends organizations inform individuals of the following:

   - the identity of the receiver or categories of receiver;
   - the country or countries to which the personal data is to be transferred;
   - why the organization needs to make a restricted transfer;
   - the type of personal data to be transferred;
   - the individual may withdraw their consent; and
   - the possible risks involved in making a transfer to a country which does not provide adequate protection for personal data and without any other appropriate safeguards in place (*e.g.*, U.K. IDTA, U.K. Addendum).

2. **Necessary To Perform a Contract Between the Individual and the Organization or Pre-contractual Steps Requested by the Individual**

   The ICO guidance gives the example of a U.K. travel company that offers bespoke travel arrangements to its customers. The company could rely on this exception to send a customer's

personal data to a hotel in Peru, provided that it does not routinely transfer its customers' personal data to said hotel. Otherwise, the U.K. travel company would be required to put an appropriate safeguard in place.

3. **Necessary To Conclude or Perform a Contract Concluded in the Interest of the Individual Between the Organization and Another Natural or Legal Person**

   Continuing with the previous example, the ICO guidance notes that the U.K. travel company could also transfer the personal data of the customer's family members to the hotel in Peru if the customer had purchased a holiday package from the U.K. travel company on behalf of their family members.

4. **Necessary To Establish a Legal Claim or Defence, or To Make or Defend a Legal Claim**

   While the claim must be legal in nature, the ICO guidance clarifies that such a claim may be brought and defended in a court or tribunal (*e.g.*, employment tribunal), and may include administrative or out-of-court procedures (*e.g.*, arbitration, mediation). Additionally, the ICO guidance explains that this derogation applies where an organization involved in the legal claim (1) is engaged in pre-action correspondence, (2) takes advice about the legal risk in bringing or defending the claim, or (3) receives a request for information from a non-U.K. regulator that intends to take formal action. In practice, this derogation is often used in the context of cross-border discovery (*e.g.*, where a U.S. court requests certain personal data relating to U.K. individuals).

5. **Necessary To Make an Exceptional Transfer Based on 'Compelling Legitimate Interests'**

   The threshold for meeting this exception is very high. As the ICO guidance notes, this exception is for "truly exceptional circumstances" where all of the following apply:

   1. The organization cannot use any valid data transfer mechanisms;
   2. None of the other exceptions apply;
   3. The transfer is not repetitive;
   4. The personal data relates to a limited number of people (though there is no absolute threshold);
   5. The transfer must be necessary for the organization's compelling legitimate interests. This means there must be serious consequences to the organization if it is unable to make the restricted transfer, or very significant benefits if the organization makes the restricted transfer;
   6. The organization's compelling legitimate interests outweigh individuals' rights and freedoms;
   7. The organization has done a full assessment of the circumstances surrounding the transfer and provided suitable safeguards to protect the personal data;
   8. The organization has informed the person whose personal data is being transferred about the restricted transfer and why its compelling legitimate interest outweighs any risk of harm to them; and
   9. The organization has informed the ICO about the transfer.

Key Takeaways

Compliance with the rules on restricted transfers (particularly in light of the CJEU ruling in *Schrems II*) is an enforcement priority for European supervisory authorities. For instance, the Spanish supervisory authority, Agencia Espanola Proteccion Datos, issued a fine of €8.5 million to a telecommunications company in 2021 for various breaches of the EU GDPR (including a €2 million penalty for transferring personal data to Peru without appropriate safeguards in place).

While the ICO guidance on international transfers and TRAs provide welcome clarity to organizations on the rules on restricted transfers, they also highlight the growing divergences between the U.K. and EU in relation to international transfers of personal data. Such divergences may become more significant in the coming months and years as the U.K. government and EC separately negotiate with countries on adequacy status, and the U.K. Data Protection and Digital Information Bill (which is set to reform the U.K. GDPR) makes its way through Parliament.

For international organizations that transfer personal data outside the U.K. and the EU, this may mean complying with two potentially conflicting (at the very least, differing) sets of requirements, resulting in more burdensome administrative work ahead of carrying out international transfers.

Return to Table of Contents

UK Information Commissioner's Office Publishes Draft Guidance on Employment Monitoring at Work

The U.K. ICO has published draft guidance on employers' monitoring of their employees at work in the U.K.

On October 12, 2022, the ICO published draft guidance titled "Employment Practice: Monitoring at Work Draft Guidance,"[13] which provides clarity to employers on the regulatory framework for monitoring employees at work. The guidance appears to be partially inspired by the recent COVID-19 pandemic and the transition to

[13] See the ICO's draft guidance.

hybrid in-office/work-from-home models. The guidance is open to consultation until January 11, 2023, but the ICO has limited the scope of the consultation to high-level feedback. As such, the ICO is unlikely to make significant changes to the guidance.

While the guidance makes it clear that any employee monitoring must be carried out lawfully and in accordance with key data protection principles (as discussed below), the key practical takeaway for employers is that they must document the need to conduct any monitoring activities with data protection by design in mind from the outset.

Overview of the Guidance

The guidance focuses on how employers can comply with the U.K. GDPR and U.K. Data Protection Act 2018 (DPA) when monitoring employees at work. The U.K. GDPR and DPA form part of the U.K.'s wider regulatory and legal framework for monitoring employees at work, which includes guidance on best practices when monitoring employees from the U.K. Advisory, Conciliation and Arbitration Service (ACAS) and the Regulation of Investigatory Powers Act 2000 (RIPA), which regulates the monitoring and other information gathering inside and outside of the workplace context.

The guidance forms part of the ICO's intention to replace the existing "Employment Practices Code," which predates the implementation of the U.K. GDPR and DPA, and to launch an online hub for employers to access guidance on data protection and employment law.

The first half of the guidance focuses on the general obligations of employers in relation to monitoring their employees. These obligations apply to systematic monitoring (*i.e.*, company-wide) and occasional monitoring (*i.e.*, response-based, specific, temporary monitoring). The second half of the guidance examines specific data protection considerations for workplace monitoring and provides practical guidance for the most common forms of employee monitoring (*e.g.*, monitoring employee phone calls, emails and biometric data). These obligations are in addition to the duty of trust and confidence, which is implied by common law into every U.K. employment agreement and requires employers to act reasonably in dealings with their employees. This duty also applies in the context of employee monitoring and overlaps with the guidance from the ICO.

Necessary and Proportionate

The overarching message of the guidance is that any monitoring of employees by an employer must be done in a manner that respects the principles of the U.K. GDPR, particularly regarding the principles of transparency, fairness and purpose limitation. The best means of achieving this is by approaching every instance of employee monitoring with a careful balancing test, whereby the business interests of the employer in monitoring are balanced against the employee's rights, freedoms and expectations in relation to their personal data. Employers must be able to justify why monitoring is necessary and proportionate to achieve a particular purpose, and determine whether there are any less intrusive means to achieve the same purpose. The guidance provides an example of using dashcams for the purposes of protecting drivers, passengers and assets, and helping to reduce insurance costs. While the use of noncontinuous video recording may be necessary and proportionate for such purposes, the use of audio is unlikely to be (except in exceptional circumstances, such as a case where a person is threatening the driver).

Legal Basis for Monitoring

An employer must have a legal basis under Article 6 of the U.K. GDPR to process employees' personal data through monitoring and a special condition under Article 9 of the U.K. GDPR for monitoring any special categories of personal data (see above).

Consent

Under the U.K. GDPR, the threshold for consent is high, outlined as freely given, specific, informed and unambiguous. The guidance notes that employers are unlikely to be able to rely on consent for employee monitoring due to the imbalance of power between an employer and employee. However, employers may be able to rely on consent where an employee consents to monitoring, having been given an alternative that can be accepted freely without any detriment to the employee from choosing such alternative. The guidance gives the example of using biometric data (*e.g.*, fingerprint scanning, facial recognition) for access control to company devices (*e.g.*, laptops). An employer can only rely on an employee's consent to the use of such biometric data for access control purposes where the employer has given the employee a reasonable alternative (*e.g.*, keycard, pin code) without any detriment to the employee from choosing such alternative.

Legitimate Interest

The guidance notes that the most "flexible" legal basis is legitimate interest. To rely on this basis, an employer must conduct a three-part test:

- **Purpose test:** Is there a legitimate interest to the processing?
- **Necessity test:** Is the processing necessary for that purpose?
- **Balancing test:** Do the employee's interests override the employer's legitimate interest?

Employers must document this analysis to be able to demonstrate that the legitimate interest applies. The best practice is to conduct a legitimate interest assessment, a template of which is available on the ICO website.[14]

Employers should note that where they are relying on legitimate interest as the legal basis for processing an employee's personal data through monitoring, the employee can object to such monitoring. The employee must provide specific and personal reasons for their objection, and the employer may refuse to comply with this objection if (1) it can demonstrate "compelling legitimate interests" that override the employee's right and freedoms, or (2) the monitoring is for establishment, exercise or defense of legal claims.

Special Categories of Personal Data

Special categories of personal data refer to personal data that relates to or concerns a person's race or ethnicity, sexual orientation, sex life, political opinions, religious or philosophical beliefs, biometric data (where used for identification purposes), genetic data and health data. If an employer monitors special categories of personal data, they must have (1) a legal basis (as discussed above), and (2) a special category condition (as set out in Article 9 of the U.K. GDPR). The special category conditions that are most likely to apply in a work setting are (1) explicit consent (this is a higher threshold than consent as a legal basis and unlikely to apply in an employer-employee relationship), (2) reasons of substantial public interest with a basis in law (*e.g.*, a bank using CCTV to detect and prevent crime), and (3) employment, social security and social protection if authorized by law (*e.g.*, monitoring to ensure the health, safety and welfare of workers).

Key Data Protection Principles

Transparency

Employers need to inform employees in advance about the nature, extent and reasons for any monitoring activities in a way that is accessible and easy to understand. Such information should be included in the company's internal privacy notice and/or employee handbook.

Covert Monitoring

Employers may only carry out covert monitoring in exceptional circumstances (*e.g.*, where necessary to prevent or detect suspected criminal activity or gross misconduct). Employers should outline in their organizational policies (made available to employees) the types of behavior that is not accepted and the circumstances in which covert monitoring may take place. If considering conducting covert monitoring, employers must (1) complete a data protection impact assessment (DPIA; see below), (2) obtain authorization from the highest authority in the workplace, (3) only conduct such monitoring on a temporary basis and within the shortest timeframe possible, (4) limit the number of people involved, and (5) set rules limiting disclosure and access to any information collected. Additionally, employers must not conduct covert monitoring in areas where employees would reasonably expect privacy (*e.g.*, restrooms) or capture communications which employees would reasonably expect to be private (*e.g.*, personal emails). Once the investigation is complete, employers must cease any covert monitoring.

Purpose Limitation

Employers must be clear about the purpose of any monitoring activities, and should document this purpose and what they intend to do with the information they collect. This information must be made available to employees (*e.g.*, via the internal privacy notice or employee handbook).

As a general rule, employers cannot change the purpose for monitoring employees unless the new purpose is (1) compatible with the original purpose, (2) related to a clear legal provision allowing the processing in the public interest, (3) done in the employee's best interests, or (4) related to an activity that no employer could reasonably ignore (*e.g.*, criminal activity at work).

Fairness

Employee monitoring must be fair, meaning employees should only be monitored in ways that they would reasonably expect and not in ways that cause unjustified adverse effects to them. The guidance provides an example of an employer installing CCTV in the employee changing rooms for the purposes of detecting and preventing thefts. As employees would reasonably expect privacy in the changing rooms, such monitoring would be unfair. However, if the employer were to (1) install CCTV to monitor the door to the changing rooms, (2) put up signs to inform employees about the camera, and (3) time-limit the CCTV recordings, such monitoring would be fair.

The guidance also warns employers about the risks of bias from using facial recognition technologies. Studies have shown that the error rates in such technologies vary depending on characteristics such as age, sex, race and ethnicity. The ICO recommends employers conduct a DPIA before using facial recognition technologies to assess whether they respect the principle of fairness.

Data Security

Employers must ensure that any personal data collected through monitoring is protected by appropriate organizational and technical measures. Employers should assess the data security risks of

[14] See the ICO's guidance on how to apply legitimate interests in practice.

monitoring to determine the appropriate security measures to put in place, and limit access to the data to those who need access and who are properly trained to handle monitoring information.

Data security is a current enforcement priority for the ICO. For example, on October 24, 2022, the ICO fined a construction company £4.4 million for failing to put appropriate security measures in place to prevent a cyberattack in which hackers accessed the personal data of up to 113,000 employees through a phishing email. Information Commissioner John Edwards warned that if organizations do not regularly monitor for suspicious activities in their systems and fail to act on warnings, they can expect to face similar fines from the ICO.

Data Minimization

Employers should not collect more data through employee monitoring than they need to achieve the purpose of such monitoring. This is closely tied to the principle of purpose limitation (see above). The guidance warns against the risks of "function creep," whereby monitoring technologies gather wider categories and larger amounts of information than necessary to achieve their purpose.

Data Protection Impact Assessments

Employers must complete a DPIA in cases where monitoring activities present a high risk to the rights and freedoms of employees (*e.g.*, covert monitoring). Even where monitoring activities do not create such high risk, the ICO recommends employers conduct a DPIA as good practice. In conducting a DPIA, employers should take into consideration the extent of employees' privacy expectations (which are likely to be greater when working from home than in the office), as well as the impact of the monitoring on the rights of employees and anyone else captured by the monitoring (*e.g.*, the general public). Additionally, best practices dictate that employers should consult employees as part of the DPIA.

According to the guidance, employers must carry out a DPIA in cases where the monitoring involves:

- the use of analytics to make inferences, predictions or decisions about employees;
- processing biometric data to uniquely identify an individual;
- the use of facial recognition technologies; and
- any covert monitoring.

Automated Processes in Monitoring Tools

The guidance recognizes the business benefits of monitoring tools with automated processes or so-called "people analytics" (*e.g.*, managing performance, monitoring absences). However, the ICO warns of the risks to employees' rights and freedoms from automated decision making (*i.e.*, decision-making without human involvement) based on automated monitoring. The guidance includes an example of an organization that bases employees' pay entirely on automated monitoring of their productivity. As such monitoring would affect how much an employee is paid, it would have a significant effect on them. Automated decision-making that has a legal or similarly significant effect on employees is subject to the rules under Article 22 of the U.K. GDPR. Employers can only make such automated decisions where the decision is (1) necessary for the entry into or performance of the employment contract, (2) authorized by the laws that apply to the employer (provided that such laws feature suitable safeguards for the employee's rights and freedoms), or (3) based on the employee's explicit consent (which is unlikely to apply in an employer-employee relationship). The ICO recommends employers give employees information about the processing, introduce simple ways for employees to request human intervention or challenge an automated decision and carry out checks to ensure that any automated decision-making tools are working as intended.

Feedback on the Guidance

Employers can provide their feedback to the guidance by downloading and completing the questionnaire on the ICO website and emailing it to employmentguidance@ico.org.uk. The deadline for submissions is January 11, 2023.

Key Takeaways

Employee monitoring is an enforcement priority for European supervisory authorities. For example, on March 31, 2022, the ICO concluded an investigation into employee monitoring by a major financial institution. While the ICO did not take enforcement action against the company, it recommended that it conduct a DPIA in relation to any employee monitoring tools used. Additionally, in 2020, Hamburg, Germany's Commissioner for Data Protection and Freedom of Information fined a worldwide clothing retailer €35.3 million for employee recording practices. In addition, the French supervisory authority, CNIL, announced that telework monitoring was one of its top three priorities for 2022.

While the final version of the guidance will not be binding, employers should familiarize themselves with its content and review their existing policies and procedures to ensure they are compliant. With the transition to hybrid in-office/work-from-home models, the use of employee monitoring tools is likely to increase, meaning the ICO and other supervisory authorities are likely to continue to monitor compliance in this area and take enforcement action where necessary.

Return to Table of Contents

Illinois Court Rules on Case Involving Retention Policy Time Limit Under the Biometric Information Privacy Act

An Illinois court has issued a ruling in *Mora v. J&M Plating, Inc.*, 2022 IL App (2d) 210692, which focused on the time limit for establishing retention policy under the Illinois Biometric Information Privacy Act (BIPA). In its ruling, the Illinois appellate court held that BIPA requires private entities to develop a retention-and-destruction schedule upon possession of biometric data. This ruling underscores the need for business collecting and using biometric data to establish retention policies *prior* to data collection.

Ruling

Section 15(a) of BIPA requires private entities in possession of biometric identifiers or biometric information (collectively, "biometric data") to develop a data retention-and-destruction schedule, which must be made available to each consumer and posted publicly.[15] BIPA does not specify when an entity must develop a schedule to satisfy section 15(a). However, on November 30, 2022, the Illinois appellate court in *Mora* concluded that a private entity must "*develop* a retention-and-destruction schedule upon *possession* of biometric data," meaning the schedule must exist at the moment an entity obtains *possession*.

Background

In September 2014, plaintiff Trinidad Mora began using his fingerprint to clock into work at defendant J&M Plating, Inc. (J&M). The company did not have a data retention-and-destruction policy developed at that time and implemented one nearly four years later. On May 22, 2018, Mr. Mora signed the company's newly developed policy and consented to the collection of his biometric data. Pursuant to defendant's policy, Mr. Mora's biometric data was destroyed soon after his employment was terminated in January 2021. One month later, Mr. Mora filed a class-action lawsuit against defendant, alleging various BIPA violations and seeking declaratory relief, injunctive relief and damages.

Mr. Mora's complaint alleged, among other things, that J&M failed to develop a written data retention-and-destruction schedule prior to collecting, storing and using its employees' fingerprint information, as required by Section 15(a) of BIPA. The company then moved for summary judgment, arguing that Section 15(a) does not specify a timetable to develop a retention-and-destruction schedule, meaning the fact that J&M did not have a schedule when Mr. Mora's biometric data was first obtained is irrelevant. J&M also argued that because the company did develop a retention-and-destruction schedule before Mr. Mora was terminated, there was no harm. The trial court agreed with J&M and granted summary judgment in its favor, finding Section 15(a) contains no timing requirement and that, regardless, J&M developed and complied with their policy before Mr. Mora was terminated, meaning there was no harm.[16]

The Appellate Court's Ruling

On appeal, Mr. Mora argued Section 15(a) required the defendant to develop a data retention-and-destruction schedule "prior to" its possession of biometric data, "or, alternatively, at the moment of possession or within a reasonable time thereafter." He reasoned that his view was consistent with legislative intent, and that allowing an entity to retroactively comply with Section 15(a) after it collects biometric data would undermine BIPA's overall scheme because no other provision allows retroactive compliance. J&M responded that Section 15(a) is meant to ensure biometric data are timely destroyed, which is why no timetable for compliance is given, further contending that as long as a schedule is in place on the day the biometric data are no longer needed or the relationship ends, then Section 15(a) is satisfied. Additionally, the company contended that because the different provisions of BIPA cover different steps in the BIPA process, having different timetables, depending on the provision, would not be unusual.

Justice Ann Jorgensen, speaking for the appellate panel, agreed with Mr. Mora and concluded that the trial court erred in granting summary judgment. The court reasoned that "section 15(a) specifies that a private entity 'in possession of' biometric data 'must' (1) 'develop a written policy,' (2) publish it, and (3) comply with it.... The explicit trigger for the *development* of the written policy (*i.e.*, the retention-and-destruction schedule) is the private entity's *possession* of biometric information." Justice Jorgensen found the court's conclusion to be consistent with BIPA's statutory scheme, which requires entities to establish BIPA-compliant procedures to protect biometric data. The court found "no rational reason" why the timeframe to develop of a data retention-and-destruction schedule would be different than Section 15(b)'s timeframe requiring notice — including how long the data will be kept —

[15] Section 15(a) provides that "[a] private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena ... , a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines." 740 ILCS 14/15.

[16] The appellate court found that the trial court erred in finding there could not be a Section 15(a) violation because Mr. Mora sustained no harm, contrary to *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186 (2019). *Id.* at *5; *see also Rosenbach* (finding that a plaintiff need not allege actual harm or adverse effect under BIPA Section 15(b) to satisfy standing in Illinois state court).

before collection. Therefore, the court concluded "that the duty to develop a schedule upon possession of the data necessarily means that the schedule must exist on that date, not afterwards."

Key Takeaways

The decision in *Mora* creates a quasi-strict liability regime for BIPA Section 15(a). Clients should therefore ensure that they develop a data retention-and-destruction schedule prior to collecting biometric data.

Return to Table of Contents

Software Company Not Covered Under Businessowners Insurance Policy for Losses Arising From Ransomware Attack

On December 27, 2022, the Supreme Court of Ohio held that software company EMOI Services, LLC (EMOI) was not entitled to coverage under its businessowners insurance policy for losses arising from a ransomware attack, reasoning that the attack did not cause the requisite "direct physical loss of or damage to" EMOI's software.[17]

The Ransomware Attack and Owners' Disclaimer of Coverage

In September 2019, a hacker unlawfully gained access to EMOI's computer systems and encrypted its files, rendering them inaccessible to the company. The hacker demanded a ransom payment of three bitcoins (approximately $35,000 at the time) in order to decrypt the files. EMOI ultimately paid the ransom, and the hacker provided a key to decrypt the files, after which the company successfully regained access to the majority of its computer systems. However, the key did not work for certain of EMOI's files, thereby rendering them permanently inaccessible. EMOI's computer systems did not sustain any hardware or equipment damage as a result of the attack.

EMOI filed a claim under its businessowners insurance policy, which provided property coverage, seeking coverage for the ransom payment and the costs associated with investigating and remediating the attack. The insurer, Owners Insurance Company (Owners), denied the claim on the basis that the policy's "Electronic Equipment" Endorsement did not apply because it requires "direct physical loss of or damage to 'media' which [EMOI] own[s]," and EMOI did not sustain any such physical loss of or damage to its media as a result of the ransomware attack.

The Coverage Dispute

In December 2019, EMOI filed suit against Owners in the Court of Common Pleas of Ohio alleging breach of contract and bad faith. The trial court ruled in favor of Owners on summary judgment, but the appellate court reversed. On Owners' appeal, the Supreme Court of Ohio reversed the appellate court's ruling, concluding that the "Electronic Equipment" Endorsement did not apply to EMOI's ransomware loss. The court first found that the endorsement was "clear and unambiguous in its requirement that there be direct physical loss of, or direct physical damage to, electronic equipment or media before the endorsement is applicable." It then proceeded to conclude that "[s]ince software is an intangible item that cannot experience direct physical loss or direct physical damage, the endorsement does not apply in this case." The court therefore reinstated the trial court's grant of summary judgment in favor of Owners and against EMOI.

Key Takeaways

The issue of whether property insurance policies, including business package policies such as the policy that Owners sold to EMOI, cover loss of or damage to computer systems inflicted with ransomware, malware and similar cyberattacks has been increasingly litigated in recent years. While some courts have determined that property policies cover such losses, other courts have concluded that they do not in the absence of an actual physical loss to the computer system. The Supreme Court of Ohio, in reliance on the plain language of the policy, adopted the latter conclusion.

The Supreme Court of Ohio's decision in *EMOI v. Owners* may be valuable for property insurers in future coverage disputes not only concerning losses arising from ransomware and other cyberattacks, but also those concerning coverage for other nonphysical losses. The decision also may cause policyholders to revisit and clarify the scope of coverage intended for such incidents under their property insurance coverage or to seek such protection via other coverage.

Return to Table of Contents

Pennsylvania Amends Its Breach of Personal Information Notification Act

Pennsylvania recently amended the state's data breach notification law to expand the definition of personal information and provide a new method for data breach notification.

On November 3, 2022, Pennsylvania Gov. Tom Wolf signed Senate Bill 696 into law, amending the state's data breach notification law to expand the definition of personal information and

[17] The decision is *EMOI Servs., L.L.C. v. Owners Ins. Co.*, No. 29128, 2021-Ohio-3942, 2022 WL 17905839 (Sup. Ct. Ohio Dec. 27, 2022).

provide a new method for data breach notification. The act will take effect on May 2, 2023.

Key changes to the law include:

1. **An expansion of the definition of "personal information."** Under the act, the definition of personal information now also includes: (1) medical information (any individually identifiable information contained in the individual's current or historical record of medical history or medical treatment or diagnosis created by a health care professional), (2) health insurance information (an individual's health insurance policy number or subscriber number in combination with access code or other medical information that permits misuse of an individual's health insurance benefits), and (3) a username or email address, in combination with a password or security question and answer that would permit access to an online account.
2. **A HIPAA exception to compliance with the law.** The act exempts from the law entities and business associates that are subject to and in compliance with HIPAA.
3. **A new permissible method of providing notice of a breach in certain circumstances.** If the affected personal information consists of a username or email address in combination with a password, electronic notice will now also be permitted, provided the notice directs the individual whose personal information has been compromised to promptly change their password and security question, or to take other steps appropriate to protect their online account.

Background

Previously, the act defined "personal information" only through: (1) a Social Security number, (2) a driver's license number or state identification number, and (3) a financial account number, credit or debit card number, along with any required security code, access code or password that would permit access to an individual's financial account. This amendment aligns Pennsylvania with many other states that have expanded the definition of personal information to include medical information and usernames. Some states have additionally included biometric information, taxpayer and IRS identification numbers, passport numbers and other identifiable information in their expanded laws.

Key Takeaways

Pennsylvania's amendment is another example of states continuing to modify their data breach notification laws to keep in line with what constitutes personal information, as well as how and when entities must provide notice. The amendment serves as an important reminder that companies need to be mindful of each state's developments in this space.

Return to Table of Contents

District Court Finds Coverage for Data Breach Losses Under Technology Professional Liability Policy

A federal district court in Minnesota recently ruled that Fishbowl Solutions, Inc. (Fishbowl), a technical consulting and software development company, is entitled to coverage for its losses arising out of a data breach from its cyber insurer, Hanover Insurance Company (Hanover).[18]

The Underlying Data Breach and Fishbowl's Insurance Claim

In November 2019, an "unknown bad actor" gained unauthorized access to the email account of a senior accountant at Fishbowl, thereby allowing the bad actor to divert client invoice payments worth nearly $177,000 to an account under the bad actor's control. Fishbowl recovered a small portion of that money and sought coverage for the remaining $148,000 under the "Cyber Business Interruption and Extra Expense" clause in its Technology Professional Liability Policy issued by Hanover. That clause stated "we will pay actual loss of business income and additional extra expense incurred by you during the period of restoration directly resulting from a data breach which is first discovered during the policy period and which results in an actual impairment or denial of service of business operations during the policy period." Hanover denied the claim.

The Insurance Coverage Dispute

Thereafter, Fishbowl filed suit in the U.S. District Court for the District of Minnesota seeking damages for breach of contract and a declaratory judgment that the company is entitled to coverage for the data breach.

The parties moved for summary judgment, which centered on the proper interpretation of the policy's Cyber Business Interruption and Extra Expense clause. Hanover argued that (1) Fishbowl did not suffer a loss of business income because (i) the clause's use of the phrase "business operations" applied only to revenue-generating activities and not client communications and billing, and (ii) Fishbowl's accrual accounting methods meant the company was seeking indemnity not for money it would have earned, but for money that Fishbowl would have received if not for the bad actor; (2) Fishbowl's loss did not *directly* result from the data breach because the decision of the company's client to send invoice payments to the bad actor rather than Fishbowl constituted an intervening action breaking the causal chain between the bad actor's conduct and Fishbowl's loss; and (3) there was

[18] The decision is *Fishbowl Solutions, Inc. v. Hanover Insurance Company*, No. 21-cv-00794 (D. Minn. Nov. 3, 2022) (ECF No. 84).

no "impairment" of Fishbowl's "business operations" because the company continued to conduct income-generating activities while the bad actor was diverting payments.

The district court granted summary judgment in favor of Fishbowl, firmly rejecting each of Hanover's arguments. First, the court found that Fishbowl did suffer a loss of business income, reasoning that the policy's definition of "business operations" was not limited to revenue-generating activities, stating "if Hanover wanted to restrict 'business operations' to include only the 'income-generating' subset of Fishbowl's 'usual and regular business activities,' it had the responsibility as drafter to write the governing contractual definition accordingly." The court further found that Fishbowl's loss directly resulted from the data breach because Fishbowl's loss would not have occurred without the bad actor accessing the Fishbowl accountant's email and sending fraudulent emails. Finally, the court concluded that Fishbowl's business was in fact impaired because, while the company's ability to communicate with its client "may not have been debilitatingly disrupted, it was certainly diminished," pointing to the fact that Fishbowl accountants could not effectively communicate with clients.

Key Takeaways

The district court's decision in favor of Fishbowl turned at least in part on the fact that Hanover did not expressly limit the "business operations" definition in its policy to revenue-generating activities. It therefore serves as an important reminder — particularly in light of the increasing frequency of data breaches and related insurance claims — that insurers and policyholders should carefully review their policies to make the parties' intentions with respect to coverage clear.

Return to Table of Contents

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000