The price of data security

A guide to the insurability of GDPR fines across Europe

May 2018

DLA PIPER

AON
Empower Results®

Table of Contents

Foreword

The General Data Protection Regulation (EU) 2016/679 (GDPR), effective from 25 May 2018, revolutionises the data protection regime and significantly affects how organisations worldwide collect, use, manage, protect, and share personal data that comes into their possession.

As personal data increasingly represents an important new class of economic asset for organisations, GDPR has significantly increased the enforcement powers available to regulators. GDPR fines can reach up to €20 million, or up to 4% of a group's annual global turnover if higher.

The scale of these fines has understandably generated concern in boardrooms. GDPR replaces a regime under which fines for a data breach were limited and enforcement actions infrequent. The regulatory environment across European Member States is undoubtedly shifting and regulators have greater powers of enforcement.

Moreover, the consequences of GDPR non-compliance are not limited to monetary fines. There are also the costs associated with non-compliance. These costs, potentially resulting from a data breach, could include for example, legal fees and litigation, regulatory investigation, remediation, public relations, and other costs associated with compensation and notification to impacted data subjects. Furthermore, the potential damage to an organisation's reputation and market position can be significant.

The magnitude of GDPR fines means organisations are keen to know whether these fines can be insured. Typical cyber insurance policies only insure fines when "insurable by law", and stipulate that the insurability of fines or penalties shall be determined by the "laws of any applicable jurisdiction that most favours coverage for such monetary fines or penalties." Organisations also need to consider other costs and liabilities that could result from GDPR non-compliance.

Given the size of the potential financial impact of GDPR non-compliance, it is important for organisations to understand how the insurability of fines, legal and other costs and liabilities following a data breach is approached in different jurisdictions. In this guide we provide an overview of the insurability of fines and resulting costs across Europe *(Information current at date of publishing)* as a resource for all those organisations affected by GDPR.

There are only a few jurisdictions where civil fines can be covered by insurance - even then there must be no deliberate wrongdoing or gross negligence on the part of the insured. Criminal penalties are almost never insurable. GDPR administrative fines are civil in nature, but the GDPR also permits European Member States to impose their own penalties for personal data violations. If those penalties are criminal, they almost certainly would not be covered by insurance.

"While there are only a few jurisdictions where GDPR fines are insurable, insurance against legal costs and liabilities following a data breach is widely available across Europe and may provide valuable cover to organisations. However, corporate groups still need to consider reputational damage and impact on existing customers, the wider market, and their relationships with regulators, all of which may go beyond quantifiable financial losses. Prevention is better than the cure."

Prakash (PK) Paran, Partner and Co-Chair, Global Insurance Sector, DLA Piper

While the insurability of fines may be limited, insurance forms a key component of an organisation's GDPR risk management strategy to manage costs associated with GDPR non-compliance and resulting business disruption losses.

In addition to insurance, there is significant business advantage to taking privacy and data protection seriously. Properly securing the data you hold is critical, but a robust data retention strategy is essential. Organisations frequently retain too much data for too long, without discernible commercial benefit; thereby increasing their organisation's risk exposure. High profile breaches and revelations regarding the misuse of data shared via social media have made consumers more aware of how their data might be collected, stored, analysed and used.

"GDPR compliance can also strengthen customer relationships. Public opinion on data privacy is changing and customers are increasingly placing importance on how organisations protect their personal information. Organisations can use regulations as opportunities to show how much they value customers. GDPR provides the chance to reinforce their role as responsible stewards of personal information and to craft innovative privacy and security policies that better reflect the constantly evolving needs of digitisation."

Vanessa Leemans, Chief Commercial Officer, Aon Cyber Solutions EMEA

This guide provides insights into the insurability of GDPR fines in different European countries' laws. It sets out findings with regard to the following:

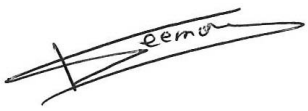
1. Insurability of non-GDPR regulatory fines
2. Insurability of GDPR fines
3. Insurability of associated costs incurred by GDPR non-compliance

Furthermore, this guide illustrates some common issues experienced by organisations through the use of international claims and data breach scenarios. It provides details of a number of professionals to contact for more information about any of the issues discussed in this guide.

We hope that you find this an invaluable guide to understanding and managing the impact of GDPR on your organisation, whilst supporting you and your stakeholders to make informed decisions.

Onno Janssen
Chief Executive Officer,
Aon Global Risk Consulting,
Aon Cyber Solutions EMEA

Prakash (PK) Paran
Partner
Co-Chair, Global Insurance Sector,
DLA Piper



Vanessa Leemans
Chief Commercial Officer,
Aon Cyber Solutions EMEA

Prof. Dr. Patrick Van Eecke
Partner
Co-Chair, Global Data Protection,
Privacy and Security Practice,
DLA Piper

GDPR at a glance

The EU General Data Protection Regulation (GDPR), effective from 25 of May 2018, replaces the existing European Data Protection Directive (95/46/EC). This new regime brings new legal rights to data subjects, while extending the scope of the responsibilities for controllers and processors. It also enhances the regulators enforcement rights to include fines of up to €20 million or, if higher, 4% of an organisation's annual global turnover.

Applicability

GDPR not only applies to organisations located within the European Union, but also to organisations that offer goods or services to, or monitor the behaviour of, European data subjects, even where those organisations are located outside of the EU.

GDPR applies to the processing of "personal data", meaning any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier. This can include any information that can be used to identify an individual; a name, an email address or a phone number, but it could also include IP addresses, job roles, employee IDs or depersonalised claims data, survey information or pension details. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about individuals.

Requirements

Some of the GDPR requirements for organisations are:

Governance and accountability - GDPR introduces a new concept of accountability, which requires organisations to be able to demonstrate compliance with GDPR. The effect of this is that all organisations need to implement a formal data protection programme to demonstrate that data protection is taken seriously and their processing activities are performed in accordance with GDPR.

More rights for data subjects - Data subjects *(an identified or identifiable natural person)* are entitled to new and enhanced rights, including a right to erasure, a right to data portability, a right to challenge certain forms of non-essential processing, and a right not to be subject to an automated decision in certain circumstances. Data subjects have more control over the processing of their personal data.

Privacy by design and by default - Organisations must take privacy risks into account throughout the process of designing a new product or service, and adopt mechanisms to ensure that, by default, minimal personal data is collected, used and retained.

Privacy risk impact assessment - Privacy risk impact assessments are required before processing personal data for operations which are likely to present higher privacy risks to data subjects due to the nature or scope of the processing operation.

Appointment of a data protection officer - Appointment of a data protection officer with expert knowledge is mandatory for public authorities and for organisations whose core activities involve the regular and systematic monitoring of data subjects on a large scale (for example, data-driven marketing activities or location tracking), or which process large amounts of special categories of personal data, such as insurers, banks and healthcare companies.

Personal data breach - Requirement to notify personal data breaches to supervisory authorities within 72 hours. In the event the incident is likely to pose a high risk to the affected individuals' rights and freedom, there is also a duty to notify those individuals of the breach. A few typical examples of personal data breach include, sending personal data to an incorrect recipient or access by an unauthorised third party, computing devices containing personal data being lost or stolen, or alteration of personal data without permission.

Processors - The processing of personal data by a processor *(the entity which processes personal data on behalf of the controller)* must be governed by a contract between the processor and the controller *(the entity which determines the purposes and means of processing of personal data)*. Furthermore, unlike the current law, GDPR imposes direct statutory obligations on processors, which means they are subject to direct enforcement by supervisory authorities, fines, and compensation claims by data subjects. In practice processors may, therefore, strongly resist the imposition of any contractual indemnity on the basis that they are subject to their own direct liability under GDPR, and argue that a more balanced apportionment of risk is appropriate (for example, a cross-indemnity), or else the replacement of an indemnity with capped liability. Alternatively, the parties may agree to allocate liability in such a way as to completely exclude GDPR indemnities and accept sole responsibility, with respect to GDPR fines, penalties and assessments, while allocating responsibility for all other non-GDPR fines related liability.

Enforcement

Higher sanctions for non-compliance - In the case of non-compliance with GDPR, the regulator may impose fines up to €20 million or, if higher, 4% of an organisation's annual global turnover. Where a data breach would involve a subsidiary of a global company, the sanction and the calculation may apply at group level. This means that the turnover of the group may be taken into account and that the parent company may be sanctioned.

Broad investigative and corrective powers - Supervisory authorities have wide investigative and corrective powers including the power to undertake on-site data protection audits and issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation - GDPR makes it considerably easier for data subjects who have suffered "material or non-material damage" as a result of a GDPR breach to claim compensation against controllers and processors. The inclusion of "non-material" damage means that individuals are able to claim compensation for emotional distress even where they are not able to prove financial loss.

Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf. Although this falls someway short of a class action right, it certainly increases the risk of group privacy claims against organisations. Employee group actions are also more likely under GDPR. Data subjects also have the right to lodge a complaint with a supervisory authority, and the right to an effective legal remedy against a controller or processor.

"It is clear that individuals are increasingly concerned about how their personal data is handled by organisations. Getting privacy right is not only about complying with the law; it should also be central to an organisation's reputation management and brand perception."

Prof. Dr. Patrick van Eecke, Partner and Co-Chair, Global Data Protection, Privacy and Security Practice, DLA Piper:

Insurance

The scope of GDPR is broader than most insurance policies which are often triggered by privacy or security incidents, whereas GDPR violations can also be triggered by non-compliance separate and apart from a privacy or security incident.

To the degree an existing insurance policy is intended to cover wrongful collection and/or usage of private data and cyber-related regulatory fines, penalties and assessments, the same intent should apply with respect to GDPR. Similarly, to the extent an existing insurance policy excludes wrongful collection and/or use of private data and excludes cyber-related regulatory fines, penalties and assessments, the same should apply with respect to GDPR.

Reviewing GDPR preparedness on an enterprise basis can increase an organisation's overall cyber resilience and help to reduce their total cost of risk – separate and apart from insurance.

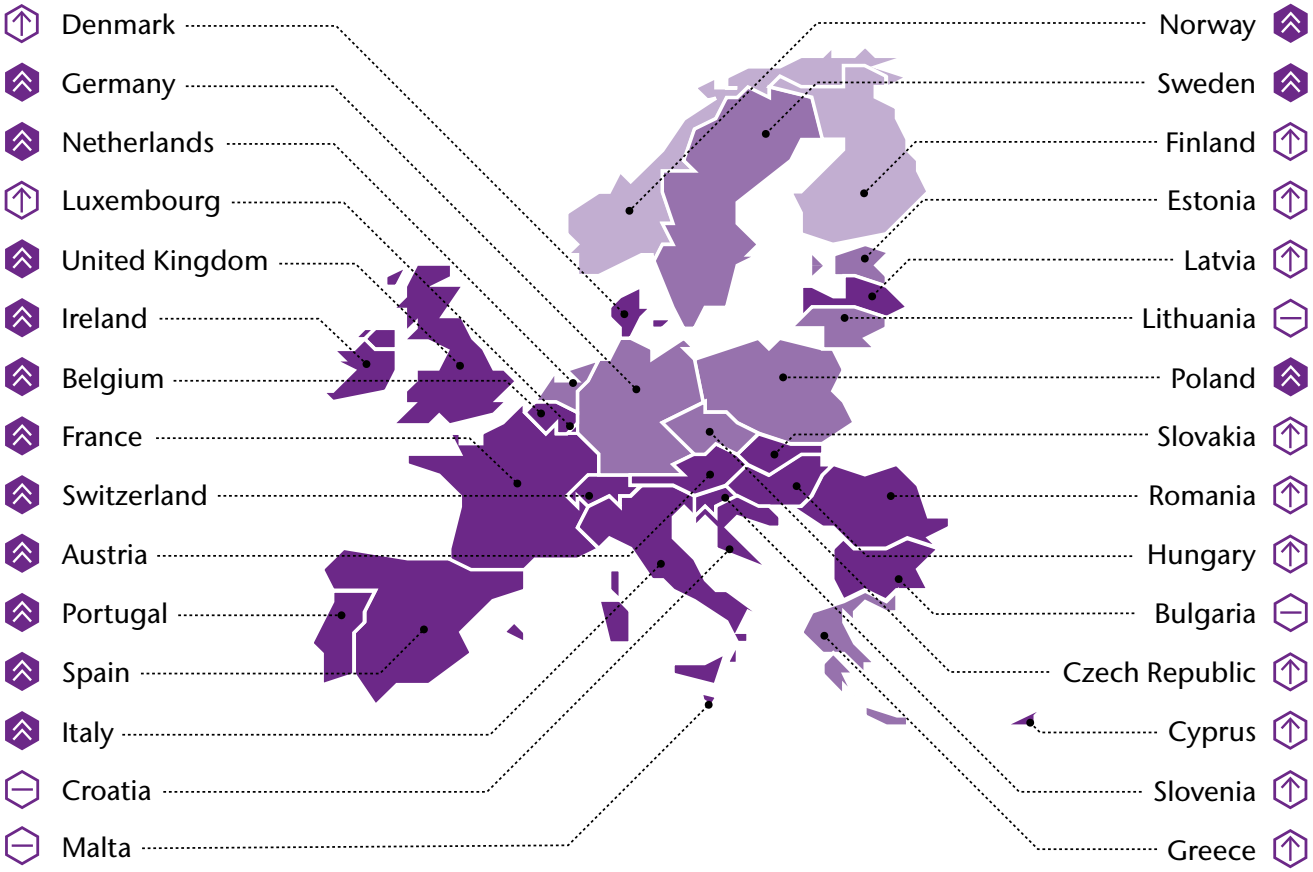
Insurability by country

DLA Piper has carried out a review of whether regulatory fines, GDPR fines in particular, and legal and other costs and liabilities following a data breach, are insurable in each EU country, Norway and Switzerland.

The findings assume that in each country local law is applied. Often it will be possible for the parties to agree that another system of law applies to an insurance contract. However, legal rules governing insurability are often derived from public policy principles which can override the parties' choice of law, meaning it cannot be assumed that such choice will prevail.

The findings also set out whether fines and other costs and liabilities are insurable "in principle" - DLA Piper has not considered whether insurance cover is available for particular risks.

GDPR heat map



Key

Insurability of GDPR fines	Insurable	Unclear	Not insurable[1]
Data regulatory environment[2]	High	Fairly high	Moderate

[1] *DLA Piper has included as "not insurable" countries where in certain limited circumstances a fine might possibly be indemnifiable, but under local laws or public policy fines would generally not be regarded as insurable*

[2] *Data regulatory environment: Presented as a metric to offer a high level guide to the approximate likelihood of exposure to regulatory action from data protection authorities, and the possible strength of that action. It is assessed through a variety of factors, including (i) availability of criminal sanctions under local law; (ii) size and historic activity level of the regulator; and (iii) presence (and complexity) of supplementary privacy and information security laws. The heat rating assigned to a jurisdiction should not be interpreted as an indication of the likelihood of that country's data protection authority commencing enforcement action in respect of any specific scenario. Importantly, GDPR is not yet a live piece of legislation, as date of publishing, and therefore we have no experience of the relative approaches of the data protection authorities to enforcing GDPR in practice.*

Source: DLA Piper

Insurability by country - overview

Jurisdiction/ system of law	Insurability of non-GDPR regulatory fines	Insurability of GDPR fines	Insurability of legal costs, other costs and liabilities following a data breach	Data regulatory environment[2]
Austria				High
Belgium				High
Bulgaria				Moderate
Croatia				Moderate
Cyprus				Fairly high
Czech Republic				Fairly high
Denmark				Fairly high
Estonia				Fairly high
Finland				Fairly high
France				High
Germany				High
Greece				Fairly high
Hungary				Fairly high
Ireland				High
Italy				High
Latvia				Fairly high
Lithuania				Moderate
Luxembourg				Fairly high
Malta				Moderate
Netherlands				High
Norway				High
Poland				High
Portugal				High
Romania				Fairly high
Slovakia				Fairly high
Slovenia				Fairly high
Spain				High
Sweden				High
Switzerland				High
United Kingdom				High

Key | **Insurability of GDPR fines**: Not insurable[1] ⬢ Unclear ⬢ Insurable ⬢

[1] *DLA Piper has included as "not insurable" countries where in certain limited circumstances a fine might possibly be indemnifiable, but under local laws or public policy fines would generally not be regarded as insurable*

[2] *Data regulatory environment: Presented as a metric to offer a high level guide to the approximate likelihood of exposure to regulatory action from data protection authorities, and the possible strength of that action. It is assessed through a variety of factors, including (i) availability of criminal sanctions under local law; (ii) size and historic activity level of the regulator; and (iii) presence (and complexity) of supplementary privacy and information security laws. The heat rating assigned to a jurisdiction should not be interpreted as an indication of the likelihood of that country's data protection authority commencing enforcement action in respect of any specific scenario. Importantly, GDPR is not yet a live piece of legislation, as date of publishing, and therefore we have no experience of the relative approaches of the data protection authorities to enforcing GDPR in practice.*

Insurability by country – detailed findings

Jurisdiction/ system of law	Insurability of non-GDPR regulatory fines	Insurability of GDPR fines	Insurability of legal costs, other costs and liabilities following a data breach
Austria	Regulatory fines are not insurable in Austria. An indemnity agreement between the offender and a third party entered into prior to the violation of regulatory provisions is considered invalid and an immoral contract.	GDPR fines are not insurable in Austria.	It is possible to insure in Austria against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. An insurer can exclude liability where there is a finding of guilt, knowledge or intent.
Belgium	Regulatory fines are generally not insurable in Belgium. Any insurance policy that purports to insure regulatory fines is likely to be considered void and unenforceable - to be borne by the party personally.	GDPR fines are not insurable in Belgium. Under draft act implementing the GDPR data protection breaches will be subject to criminal fines - criminal fines are prohibited from being insured - and must be borne by the liable party personally.	It is possible to insure in Belgium against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. An insurer can exclude its contractual liability under a policy where the insured intentionally caused the covered losses.
Bulgaria	Regulatory fines would not be insurable in Bulgaria. A claim for indemnity is likely to be unenforceable as a matter of public policy because criminal liability is personal in Bulgaria. The Bulgarian Financial Supervision Commission (FSC) would be likely to impose a fine on an insurance company which offered insurance against administrative penalties.	GDPR fines would not be insurable in Bulgaria. GDPR breaches are subject to administrative and criminal fines.	In Bulgaria, a claim under a policy for an insured's investigation and defence costs is not enforceable - it is the role of the court to rule which party will pay the costs. It may be possible to insure against: claims by third parties (customers/suppliers/data subjects) for consequences of breach, and costs of mitigating a breach - including public relations expenses.

Key | Insurability of GDPR fines — Insurable — Unclear — Not insurable

Jurisdiction/ system of law	Insurability of non-GDPR regulatory fines	Insurability of GDPR fines	Insurability of legal costs, other costs and liabilities following a data breach
Croatia	Regulatory fines would not be insurable in Croatia as they would represent a legally impermissible risk.	GDPR fines would probably not be insurable in Croatia. It is uncertain how GDPR breaches are categorized. However, GDPR fines are likely to be uninsurable as they would represent a legally impermissible risk.	It is possible to insure in Croatia against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. However, such costs are unlikely to be insurable if the action giving rise to the liability for the fine is intentional or a consequence of gross negligence.
Cyprus	Regulatory fines are not likely to be insurable in Cyprus. There is no express general prohibition in statutes and rules regulating the insurability of regulatory/ administrative fines. However, such fines are likely to be found uninsurable as a matter of public policy.	GDPR fines are not likely to be insurable in Cyprus. Adminstrative fines under GDPR are not likely to be insurable as a matter of public policy. (Cyprus courts follow English law as persuasive). This is also the case for criminal fines in relation to GDPR, should such fines be adopted under national law.	It is possible to insure in Cyprus against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses.
Czech Republic	Regulatory fines may be insurable in the Czech Republic. Insurance against regulatory fines is not expressly prohibited, but there is a risk that such contracts will be unenforceable as a matter of public policy.	GDPR fines may be insurable in the Czech Republic. Insurance against GDPR fines is not expressly prohibited, but there is a risk that such contracts will be unenforceable as a matter of public policy.	It is possible to insure in the Czech Republic against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses.

Jurisdiction/ system of law	Insurability of non-GDPR regulatory fines	Insurability of GDPR fines	Insurability of legal costs, other costs and liabilities following a data breach
Denmark	Regulatory fines are not likely to be insurable in Denmark. It is not possible to insure against criminal sanctions as a matter of public policy. This rule also applies to insurance covering regulatory fines, based on the principle that a fine must be borne by the party committing the criminal act.	GDPR fines are not insurable in Denmark. GDPR breaches will result in criminal fines. The general rule that a party cannot insure against such fines, nor claim indemnity for them.	It is possible to insure in Denmark against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. Unless it is otherwise clearly stated, a policy will not cover costs that are due to a wilful act or gross negligence.
Estonia	Regulatory fines may be insurable in Estonia. Insurance contracts covering administrative or criminal fines are not expressly prohibited, but there is a risk such contracts will be declared contrary to overriding rules of law/public order/ morality. A policy may be unenforceable if it is considered that the parties' intention was to avoid administrative or criminal sanctions. It is a condition of insurability that the loss was caused by circumstances beyond the control of the insured.	GDPR fines may be insurable in Estonia. Breaches of GDPR are sanctioned by administrative and criminal fines. There is a risk that contracts insuring against those fines will be unenforceable.	It is possible to insure in Estonia against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. However one of the conditions of insurability in Estonia is that the loss was caused by circumstances beyond the control of the insured.
Finland	In Finland there is no statutory prohibition against agreeing to indemnify regulatory fines.	GDPR fines are insurable in Finland but deliberate or grossly negligent conduct is not covered.	It is possible to insure in Finland against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. Such sums are insurable even if the insured has been found guilty - gross negligence or intentional actions prevent or decrease payable compensation.

Key — Insurability of GDPR fines

Not insurable

Unclear

Insurable

Jurisdiction/ system of law	Insurability of non-GDPR regulatory fines	Insurability of GDPR fines	Insurability of legal costs, other costs and liabilities following a data breach
France	Regulatory fines are generally not insurable in France. Insurance against fines is contrary to public policy as such coverage would tend to diminish their deterrent effect.	GDPR fines are not insurable in France. Such fines are considered to be quasi-criminal and insurance against them is against public policy as they are intended to be borne by the party personally.	It is possible to insure in France against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. Insurance would not respond if there is a finding of knowledge, recklessness or intent. There would be no underlying aleatory event (i.e. no risk) and therefore no possibility of insuring it.
Germany	Regulatory fines are likely to be uninsurable in Germany. There is no express bar but generally civil law does not allow the purpose of a fine as a personal sanction to be circumvented.	GDPR fines are likely to be uninsurable in Germany.	It is possible to insure in Germany against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. Insurance is not available where there is a finding of intent and/or recklessness.
Greece	Regulatory fines may be insurable in Greece. A claim for indemnity for regulatory fines is generally considered to be unenforceable as a matter of public policy. However, regulatory fines could be insurable to the extent the fine is not attributed to malice; and the acts or omissions which resulted in the fine do not constitute a criminal offence which has resulted or will result in the imposition of criminal sanctions. Criminal sanctions cannot be insured against, as a matter of public policy.	GDPR fines could be insurable in Greece. Under Greek law, regulatory GDPR fines could be insurable if the fine is not attributed to malice and that the acts or omissions concerned are not criminal offenses which have resulted or will result in criminal sanctions.	It is possible to insure in Greece against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. Such costs can be insured against - provided conduct giving rise to them was not a result of malice.

Jurisdiction/ system of law	Insurability of non-GDPR regulatory fines	Insurability of GDPR fines	Insurability of legal costs, other costs and liabilities following a data breach
Hungary	Regulatory fines are not insurable in Hungary. Insurance policies against such fines would be considered to be against the law, and therefore null and void.	GDPR fines are not insurable in Hungary. It is most likely that GDPR breaches are subject to uninsurable administrative (and criminal) fines.	It is possible to insure in Hungary against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. Claims under policies for such costs are enforceable - at least until it is demonstrated (e.g. by an admission or judgment) that the conduct giving rise to liability for a fine was deliberate or reckless.
Ireland	Regulatory fines are not generally insurable in Ireland. A claim for indemnity is likely to be unenforceable as a matter of public policy. A party is not allowed to claim an indemnity for criminal or quasi-criminal fines which the law has provided should be borne by the party personally.	GDPR fines are not likely to be insurable in Ireland. Under proposed legislation GDPR breaches will be subject to administrative fines and criminal fines which will be uninsurable as a matter of public policy.	It is possible to insure in Ireland against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. A claim under a policy will be enforceable - until it is demonstrated (e.g. by an admission or judgment) that the insured's conduct was deliberate or reckless
Italy	Regulatory fines are not insurable in Italy. Administrative fines are not insurable because the deterrent effect of fines would be lost if the offender could shift its economic burden to the insurer.	GDPR fines are not insurable in Italy.	It is possible to insure in Italy against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. An insurer will not be liable for payment of indemnity if loss was intentionally caused by the insured.

Key — Insurability of GDPR fines

Not insurable

Unclear

Insurable

Jurisdiction/ system of law	Insurability of non-GDPR regulatory fines	Insurability of GDPR fines	Insurability of legal costs, other costs and liabilities following a data breach
Latvia	Regulatory fines are probably not insurable in Latvia. Insurance contracts covering administrative or criminal fines are not expressly prohibited. However, such contracts may be declared contrary to overriding rules of law/ public order/ morality, or objectionable on the basis that they are aimed at avoiding legal sanctions. It is a condition of insurability that the loss was caused by circumstances beyond the control of the insured. Theoretically there might be specific and limited cases where administrative fines are insurable, but in practice this is unlikely.	GDPR fines are probably not insurable in Latvia. Breaches of GDPR are sanctioned by administrative and criminal fines. Insurance contracts covering administrative or criminal fines are not expressly prohibited. However, such contracts may be declared contrary to overriding rules of law/ public order/ morality, or objectionable on the basis that they are aimed at avoiding legal sanctions. It is a condition of insurability that the loss was caused by circumstances beyond the control of the insured. Theoretically there might be specific and limited cases where administrative fines are insurable, but in practice this is unlikely.	It is possible to insure in Latvia against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. However, one of the conditions of insurability in Latvia is that the loss was caused by circumstances beyond the control of the insured.
Lithuania	Regulatory fines may be insurable in Lithuania. Insurance contracts covering administrative or criminal fines are not expressly prohibited, but there is a risk such contracts will be declared contrary to overriding rules of law/ public order/ morality. A policy may be unenforceable if it is considered that the parties' intention was to avoid administrative or criminal sanctions. It is a condition of insurability that the loss was caused by circumstances beyond the control of the insured.	GDPR fines may be insurable in Lithuania. Breaches of GDPR are sanctioned by administrative and criminal fines. There is a risk that contracts insuring against those fines will be unenforceable.	It is possible to insure in Lithuania against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. However, one of the conditions of insurability in Lithuania is that the loss was caused by circumstances beyond the control of the insured.

Jurisdiction/ system of law	Insurability of non-GDPR regulatory fines	Insurability of GDPR fines	Insurability of legal costs, other costs and liabilities following a data breach
Luxembourg	Regulatory fines are not insurable in Luxembourg. A claim for indemnity is likely to be unenforceable as a matter of public order. Indemnity is not permitted for criminal or quasi-criminal fines, which the law has provided should be borne by the party personally.	GDPR fines are not insurable in Luxembourg. GDPR breaches are subject to administrative and criminal fines which are intended to be borne by the relevant party.	It is possible to insure in Luxembourg against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses.
Malta	Regulatory fines are unlikely to be insurable in Malta. A claim for non-GDPR regulatory fines is likely to be unenforceable as a matter of public policy.	GDPR fines are unlikely to be insurable in Malta. GDPR breaches are subject to both administrative and criminal fines, and are likely to be uninsurable as a matter of public policy.	It is possible to insure in Malta against: (i) costs of investigating an incident (ii) defence costs (iii) civil claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. A claim under a policy for such costs is likely to be enforceable - provided the insured's conduct is not intentional or grossly negligent.
Netherlands	Regulatory fines may not be insurable in the Netherlands. There is no specific legislation or case law relevant to the insurability of non-GDPR regulatory fines. A claim for indemnity is unenforceable if the claim is contrary to public policy or accepted principles of morality. Malicious intentional acts cannot be insured against.	GDPR fines may not be insurable in the Netherlands.	It is possible to insure in the Netherlands against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. A finding of guilt, recklessness, knowledge or intent (e.g. by an admission or judgment) is generally excluded from insurance coverage.

Key — Insurability of GDPR fines: Not insurable | Unclear | Insurable

Jurisdiction/ system of law	Insurability of non-GDPR regulatory fines	Insurability of GDPR fines	Insurability of legal costs, other costs and liabilities following a data breach
Norway	Regulatory fines may not be insurable in Norway. It is not permitted to enter into insurance contracts which are "in breach of the law or decency", and offering insurance cover for fines imposed for criminal sanctions could be in breach of this rule. However, regulatory fines might not be treated as criminal sanctions if the fine has no punitive purpose, in which case insurance cover would be available.	GDPR fines are insurable in Norway. Under proposed Norwegian legislation GDPR breaches will not be subject to criminal sanctions. (Justice Department proposition on page 4) Breaches will be met with regulatory fines for violations or compulsory fines. As regulatory fines are not defined as 'criminal sanctions' in the GDPR proposed legislation, insurance companies can offer insurance cover, in accordance with the Norwegian Insurance Operations Act section 7-1.	It is possible to insure in Norway against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. However, the insured's intentional or wilful acts insurable according to the Norwegian Insurance Contracts Act, section 4-9. If an insurer has covered costs resulting from intentional acts it has the right to recover from the insured.
Poland	Regulatory fines may be insurable in Poland. Criminal fines are not insurable. Administrative fines are generally considered to be insurable but the position has not been tested in court, and the court or a regulator could come to a different view.	GDPR fines may be insurable in Poland. Both administrative and criminal fines will be available as sanctions for breach of GDPR. Criminal fines will not be insurable. Administrative fines would generally be considered to be insurable, but this position has not been tested in court, and the court or a regulator could come to a different view.	It may be possible to insure in Poland against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. A claim under a policy for such costs and liabilities is enforceable until it is demonstrated (for example by an admission or judgment) that the conduct giving rise to liability for a fine was deliberate or reckless.
Portugal	Regulatory fines are not insurable in Portugal. Insurance contracts covering risks relating to liability arising from administrative offences and criminal liability are prohibited by law.	GDPR fines are not insurable in Portugal. GDPR legislation will probably include administrative offences and criminal liability - insurance contracts covering these risks are prohibited by law.	In Portugal, it is possible to insure against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses.

Jurisdiction/ system of law	Insurability of non-GDPR regulatory fines	Insurability of GDPR fines	Insurability of legal costs, other costs and liabilities following a data breach
Romania	Regulatory fines are not likely to be insurable in Romania. Insurance for fines is likely to be unenforceable as a matter of public policy. The subject matter of an insurance policy must not be prohibited by law or contrary to public order or good morals.	GDPR fines are not likely to be insurable in Romania. GDPR breaches will be subject to administrative fines, which are likely to be considered uninsurable risks, as a matter of public policy.	It is possible to insure in Romania litigation and arbitration defence costs. A claim under such a policy is enforceable - provided the insured's conduct was not intended or committed with gross negligence. Costs incurred when appealing against a decision issued by an investigation authority might also be insurable under a Legal expenses policy. In principle it is also likely to be possible to insure against claims by third parties (e.g. customers/ suppliers/data subjects) for consequences of a breach, and mitigation costs.
Slovakia	Regulatory fines are probably not insurable in Slovakia. There is no statutory basis for such insurance in the Slovak Act on Insurance and the view of the regulator is unknown. Fines for deliberate acts would lack the "randomness" required by Slovak insurance case law.	GDPR fines are probably not insurable in Slovakia.	Insuring the costs of legal representation for administrative or regulatory investigations is possible in Slovakia. It is also possible to insure against liability to third parties.
Slovenia	Regulatory fines may be insurable in Slovenia, depending on the nature of the fine. In criminal and quasi-criminal (administrative) cases, where the law provides that a fine is borne by the party itself, insurance for such fines would be deemed contrary to public order.	GDPR fines are not insurable in Slovenia. GDPR breaches are subject to both administrative and criminal fines, which are intended to be borne by the relevant party.	It is possible to insure in Slovenia against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. Costs incurred in regulatory investigations can be covered by insurance - unless liability arises as a consequence of an intentional or negligent act.

Key | Insurability of GDPR fines — Insurable — Unclear — Not insurable

Jurisdiction/ system of law	Insurability of non-GDPR regulatory fines	Insurability of GDPR fines	Insurability of legal costs, other costs and liabilities following a data breach
Spain	Regulatory fines are not currently insurable in Spain. Insurance of criminal and regulatory fines is considered to be against public policy. This position has been questioned in relation to regulatory fines by some in the Spanish insurance sector, but the Spanish regulator not changed its official position to date.	GDPR fines are not currently insurable in Spain.	It is possible to insure in Spain against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. However, losses arising from conduct entailing bad faith by the insured or deliberately caused by the insured are excluded.
Sweden	Regulatory fines may be insurable in Sweden. There is no clear statutory prohibition. The general view is that insurability depends on the character of the penalty or fine and in particular whether imposition of a penalty or fine requires intent or only negligence, or neither, from policyholder.	GDPR fines may be insurable in Sweden. The specific nature of the fine imposed and the conduct of the insured would need to be considered.	It is possible to insure in Sweden against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers/data subjects) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses.
Switzerland	Regulatory fines are generally not insurable in Switzerland. According to the Swiss Federal Supreme Court, fines of punitive nature are generally not considered compensable damages and cannot be insured.	GDPR fines are generally not expected to be insurable in Switzerland. If GDPR fines are considered to have punitive nature, claims for indemnity will most likely not be enforceable. However, Swiss law might regard an excessively high GDPR fine as violating Swiss "ordre public". In that case it is possible that the fine, or the part of it considered excessive, could be the indemnified under a policy.	In Switzerland, there are no statutory limitations with regard to the insurability of legal costs and other costs following a data breach. For example, the following costs can be insured in Switzerland: (i) defence costs (ii) claims and demands of third parties (iii) costs for consequences of breach such as data loss, breakdown of operations (iv) costs for crisis management and other mitigation costs.

Jurisdiction/ system of law	Insurability of non-GDPR regulatory fines	Insurability of GDPR fines	Insurability of legal costs, other costs and liabilities following a data breach
United Kingdom	 Regulatory fines are generally not insurable in the UK. A claim for indemnity is likely to be unenforceable as a matter of public policy. A party is not generally allowed to claim an indemnity for criminal or quasi-criminal fines which the law has provided should be borne by the party personally. FCA rules prohibit attempts to insure against FCA fines.	 GDPR fines are not expected to be insurable in the UK. Although there are rare case law exceptions to the public policy rule against indemnity, they are not expected to apply to the administrative and criminal fines that will be imposed under proposed legislation.	 It is possible to insure in the UK against: (i) costs of investigating an incident (ii) defence costs (iii) claims by third parties (customers/suppliers) for consequences of breach (iv) costs of mitigating a breach - including public relations expenses. Claims under a policy for such costs would be insurable unless it has been demonstrated (e.g. by an admission or judgment) that the conduct giving rise to liability for a fine was deliberate or reckless.

Common issues in international cyber scenarios

Scenario

"If a hotel group with headquarters in New York had hotels in France and there was a hack into the database in France, which affected Personally Identifiable Information (PII) of people in various countries, under what applicable law would a cyber insurance policy respond to such a breach? Would it be beholden to the regulations in the country where the attack happened or originated, where the data was warehoused, or does it depend on where the original customer is from?"

Different local country laws & regulations may apply to how a cyber policy will respond, depending upon the unique circumstances in each case.

What law will apply to the policy?
Courts in most EU countries will apply the Rome I Regulation (Regulation (EC) 593/2008) to determine what country's law applies to an insurance contract. If the policy covers a "large risk" (applying tests by reference to balance sheet, turnover, and number of employees) the applicable law will generally be that chosen by the parties, or if no law has been chosen, the law of the insurer's country of residence.

If the hotel group's relevant policies do not cover a "large risk", more complex rules apply under Rome I. Broadly, the parties can choose the law of any EU Member State where the risk is situated, or the law of the country of habitual residence of the policyholder, or (if the policyholder pursues commercial or industrial activity and the insurance contract covers multiple risks relating to those activities situated in different Member States), the law of one of the Member States concerned. If there has been no valid choice of law in accordance with Rome I the policy will be governed by the law of the Member State in which the risk is situated.

Jurisdictions where Rome I does not apply may approach applicable law differently. However, importantly, many countries' courts will reserve to themselves the right not to apply a system of law other than their own, if doing so would result in an outcome contrary to local rules of public policy. Rome I itself allows provisions of a foreign law to be disapplied if they are manifestly incompatible with local public policy.

As indicated by DLA Piper's review, in many European jurisdictions local laws making fines uninsurable are based on principles of morality and public policy. Drafting a policy so that it is stated to be subject to the laws of a country where fines are, or may be, insurable will not therefore guarantee that the policy responds to such fines.

A variety of different laws might therefore need to be applied to determine policy response. These will include: the applicable laws chosen in the hotel group's primary policy and any local policies; the laws in any jurisdiction where corporate policyholders (group companies) or operations are situated; and laws and public policy rules in any jurisdiction where an insurer might become involved in proceedings, e.g. if it is joined into a liability claim brought by a locally resident claimant.

What laws and regulations apply to a data breach and associated claims?
The following country laws could all be relevant (more than one may apply): laws of the country where the incident occurs (France, in the case described above); laws of every country where an individual, corporate or governmental entity resides if its data is impacted (Aon has serviced PII legal issues in over 100 countries in some cases); laws of the country where the insured is headquartered; and/or laws of the principal place of business of the insured.

The changing landscape of international privacy laws and the evolving approach of regulators can create challenges for any organisation operating on a global platform. Compliance with laws and the jurisdictional competence of a regulator can be dictated by: where the organisation is domiciled; the countries/jurisdictions in which the

organisation does business (holds/transfers data); and/or the countries/jurisdictions in which the organisation's customers/clients reside.

This is a dynamically changing environment. The *DLA Piper Data Protection Handbook* sets out an overview of the key privacy and data protection laws and regulations across nearly 100 different jurisdictions.

The choice of law and jurisdiction in a cyber insurance policy can make a difference. When claims involve fines and penalties that may be uninsurable in certain jurisdictions, insurability of GDPR fines will depend on applicable national data protection and insurance laws.

Although there may be very limited circumstances where an insured organisation is allowed to be indemnified for GDPR fines, it is clear that a cyber insurance policy can still be very beneficial to an organisation dealing with a breach of the GDPR.

Subject to the terms and conditions of the policy, a cyber insurance policy can generally cover: the costs associated with the regulatory investigation; the costs incurred in complying with the onerous notification requirements in all jurisdictions; the legal costs and compensation claims brought against an insured organisation due to an infringement of the GDPR; and/or the costs incurred to mitigate the impact on an organisation's reputation following an infringement of the GDPR.

Scenario

"A manufacturer with headquarters in Sao Paolo hired a German marketing company to conduct a marketing campaign to launch their products in Europe. The contractual arrangement between both parties does not contain any data protection terms. In order to develop a targeted marketing campaign, the marketing company first conducts some research on the existing European consumer data of the Brazilian manufacturer. It turns out that the marketing company also transferred the consumer data illegally to their Chinese branch to develop a marketing campaign for a Chinese competitor. The German regulator discovers this illegal use of data and fines the Brazilian manufacturer."

GDPR non-compliance by processor: An organisation, domiciled outside the EU, acting as controller may get fined (or incur liability) because one of its processors infringed upon the GDPR.

The processing of European consumers' personal data by the German marketing company should have been governed by a data processing agreement with the Brazilian manufacturer. Under the GDPR, the Brazilian manufacturer which acts as controller can be fined for the illegal data transfer to China and unlawful use of the data by the German marketing company.

The German marketing company will also be liable for the damages caused by the processing as it has not complied with obligations of the GDPR that are specifically directed to processors regarding the lawful international transfers of personal data.

Any European consumer who has suffered material or non-material damage (including emotional distress) as a result of an infringement of the GDPR (the illegal transfer to China and unlawful use of their personal data) shall have the right to receive compensation from the German marketing company and the Brazilian manufacturer for the damage suffered.

Where one of the parties (as either a controller or a processor) has been held fully liable to a data subject for damage which the data subject has suffered, there is a statutory mechanism under the GDPR which allows that party to claim a contribution to the costs of the compensation from another party, where that other party was also involved in the processing and was partly responsible for the damage.

An insurance policy would probably not cover the GDPR fines imposed on the Brazilian manufacturer and/or the German marketing company. Subject to the terms and conditions of the insurance policy wording, it could potentially cover the costs associated with the regulatory investigation of the German regulator, the costs of the notification to the consumers affected, the legal costs and the compensation claims brought against both parties due to the breach.

Scenario

"A company with headquarters in Finland (where GDPR fines are insurable) hires a service provider (as its processor) with headquarters in Italy to design and administer a biometric access system for the Finnish company's offices throughout Europe, including hosting of the data collected by the access system on the service provider's servers in Italy. It transpires that the access system collects unnecessary personal data, does not allow for personal data to be restricted or erased, and has weak data security. This is uncovered when a whistle-blower working for the service provider reports the deficiencies to the regulator in both countries"

In this scenario, there have likely been breaches of at least the following GDPR requirements: the data minimisation principle, the data protection by design and by default requirement and the security of processing requirement.

The first two of these are obligations of the controller, and not the processor. Therefore, the Finnish company, as controller, will be liable to supervisory authorities (in respect of administrative fines) and to data subjects (in respect of civil claims) for these breaches, notwithstanding that they were caused by its processor. However, if the contract with the service provider has been well drafted, there may be a contractual recourse for the Finnish company against the service provider as a result of the service provider doing something to put the company in breach of its obligations under data protection laws.

The security of processing requirement applies to both controllers and processors. Therefore, a supervisory authority would assess the degree of responsibility of the Finnish company and the Italian service provider, and fine them accordingly. Equally, a data subject could bring a claim directly against the service provider and could also bring a claim against the company, if it had any responsibility for the breaches, for the full amount of loss suffered by the data subject, leaving the company to seek a contribution from the processor.

Appropriate supervisory authority to lead on any enforcement action. This is a circumstance of cross-border processing as there are multiple European offices where the access system is collecting data, which is hosted in another Member State, i.e. Italy. For enforcement pursued against the Finnish company, the company can expect that its lead supervisory authority (almost certainly the Finnish data protection authority) takes charge, whilst co-ordinating with supervisory authorities in other impacted Member States.

If a claim for indemnity in respect of a fine is made by the Finnish company under a Finnish law governed insurance policy which covers GDPR fines, the Finnish company should be able to enforce that claim in the Finnish courts, assuming it has not been grossly negligent or acted deliberately. If a dispute under the Finnish company's policy is heard in another jurisdiction, it is possible that the court would refuse to enforce the claim on public policy grounds. The Italian company would not be able to enforce a claim for indemnity for the fine imposed on it under an Italian law governed policy in the Italian courts.

In both countries, investigation costs, defence costs, liability for claims brought by data subjects, and costs of mitigating the consequences of a breach (i.e. PR expenses) are potentially insurable under local law. However, in Finland, gross negligence or deliberate conduct by the insured would bar or reduce the amount of a claim under a policy, and in Italy an insurer will not be liable if the loss was intentionally caused by the insured.

Next steps

There is no doubt that GDPR is a continuous challenge for organisations, but there are steps that you can take to help manage the potential impact through risk governance, insurance review and incident response.

- Carry out a security audit to check personal data is secure against unauthorised access or processing
- Put in place a plan for ensuring continuous monitoring and follow up of data compliance efforts
- Ensure contracts with all third party processors contain at least the minimum terms stipulated by GDPR
- Adopt a privacy-by-design methodology when initiating new projects or developing new tools

- Ensure adequate cyber insurance coverage is in place
- Review your existing insurance coverage for GDPR non-compliance, especially fines, penalties and lawsuits with assistance from qualified coverage counsel

- Ensure you have an incident response plan in place, including data security breach notification procedures
- Review your existing enterprise-wide incident response plan to ensure that it incorporates escalation plans and nominated advisors covering all required stakeholders. This includes business operations, legal, PR, and key third parties such as IT service providers.

"Whilst GDPR will have a positive impact on the privacy of EU citizens, there's great concern about the financial impact to organisations. This is not a one-time event; it will require ongoing effort to manage the implications of GDPR. Organisations can protect themselves by taking an enterprise-wide approach to help achieve cyber resilience, and meet the expectations of their customers and shareholders. We hope this guide supports your organisation to do just that."

Onno Janssen, Chief Executive Officer, Aon Global Risk Consulting & Aon Cyber Solutions EMEA

Contacts

Please contact Aon Cyber Solutions for cyber security, risk and insurance expertise and DLA Piper and its relationship firms, who have carried out the insurability by country review, for legal advice.

Authors

Onno Janssen
Chief Executive Officer
Aon Global Risk Consulting,
Aon Cyber Solutions EMEA
+49 (0) 40 3605 3608
onno.janssen@aon.de

Vanessa Leemans
Chief Commercial Officer
Aon Cyber Solutions EMEA
+44 (0) 20 7086 4465
vanessa.leemans@aon.co.uk

Prakash (PK) Paran
Partner
Co-Chair, Global Insurance Sector
DLA Piper
+44 (0)20 7153 7529
pk.paran@dlapiper.com

Prof. Dr. Patrick Van Eecke
Partner
Co-Chair, Global Data Protection,
Privacy and Security Practice
DLA Piper
+32 (0) 2 500 1630
patrick.vaneecke@dlapiper.com

Aon Cyber Solutions

Kevin P. Kalinich, Esq.
Global Cyber Insurance Practice Leader
+1 312 381 4203
kevin.kalinich@aon.com

Adam Peckman
Global Cyber Risk Practice Leader
+44 (0)7803 695 386
adam.peckman@aon.co.uk

Spencer Lynch
Managing Director
Stroz Friedberg
+44 (0)20 7061 2304
slynch@strozfriedberg.co.uk

David Molony
UK Cyber Risk Practice Leader
+44 (0)777 5227008
david.molony@aon.co.uk

Shannan Fort
Global Broking Centre
Cyber Product Leader
+44 (0)20 7086 7135
shannan.fort@aon.com

Andrew Mahony
Cyber Insurance Leader Asia
+65 (0) 6313 7080
andrew.mahony@aon.com

Fergus Brooks
Cyber Insurance Leader Australia
+61 (02) 9253 7835
fergus.brooks@aon.com

Brian Rosenbaum LL.B
Cyber Insurance Leader Canada
+1 416 868 2411
brian.rosenbaum@aon.ca

DLA Piper GDPR Contacts

Austria
Sabine Fehringer
Partner
Intellectual Property & Technology
+43 (0) 153 1781 460
sabine.fehringer@dlapiper.com

Belgium
Patrick van Eecke
Partner
Co-Chair, Global Data Protection, Privacy and Security
+32 (0) 2 500 1630
patrick.vaneecke@dlapiper.com

Bulgaria
Andrey Aleksandrov
Partner
+359 (0) 2 986 9999
a.alexandrov@kambourov.biz

Croatia
Saša Divjak
Partner
Corporate
+385 (0) 1 5391 600
sasa.divjak@dtb.hr

Cyprus
Michalis Michael
Partner
Litigation & Data Protection
+357 (0) 22 459345
mm@cohalaw.com

Denmark
Marlene Winther Plas
Partner
Intellectual Property & Technology
+45 (0) 3334 0047
marlene.plas@dlapiper.com

Estonia
Mihkel Miidla
Partner
Data Protection
+372 (0) 6 400 959
mihkel.miidla@sorainen.com

Finland
Markus Oksanen
Partner
Intellectual Property & Technology
+358 (0) 9 4176 0431
markus.oksanen@dlapiper.com

France
Denise Lebeau-Marianna
Partner
Intellectual Property & Technology
+33 (0) 1401 52 498
denise.lebeau-marianna@dlapiper.com

Germany
Jan Pohle
Partner
Intellectual Property & Technology
+49 (0) 221 277 277 390
jan.pohle@dlapiper.com

Greece
Takis Kakouris
Partner
Corporate
+30 (0) 210 6967 097
t.kakouris@Zeya.com

Hungary
Csaba Vari
Senior Associate
Intellectual Property & Technology
+36 (0) 1510 1113
csaba.vari@dlapiper.com

Ireland
Claire Morrissey
Partner
Corporate
+35 (0) 3 1649 2246
cmorrissey@algoodbody.com

Italy
Giulio Coraggio
Partner
Intellectual Property & Technology
+39 (0) 02 80 618 619
giulio.coraggio@dlapiper.com

Latvia
Ieva Andersone
Senior Associate
Data Protection
+371 (0) 67 365 000
ieva.andersone@sorainen.com

Lithuania
Daivis Švirinas
Partner
Data Protection
+370 (0) 52 685 040
daivis.svirinas@sorainen.com

Luxembourg
Olivier Reisch
Partner
Intellectual Property & Technology
+35 (0) 226 2904 2017
olivier.reisch@dlapiper.com

Malta
Antoine Camilleri
Partner
Intellectual Property & Technology
+356 (0) 2540 3404
antoine.camilleri@mamotcv.com

Netherlands
Richard van Schaik
Partner
Intellectual Property & Technology
+31 (0) 20 541 9828
richard.vanschaik@dlapiper.com

Norway
Petter Bjerke
Partner
Corporate
+47 (0) 2413 1654
petter.bjerke@dlapiper.com

Poland
Ewa Kurowska-Tober
Partner
Intellectual Property & Technology
+48 (0) 22 540 7402
ewa.kurowska-tober@dlapiper.com

Portugal
Joao Costa Quinta
Partner
Litigation & Regulatory
+351 (0) 213 583 668
joao.quinta@dlapiper.com

Romania
Ana-Maria Andronic
Counsel
Intellectual Property & Technology
+40 (0) 372 155 816
anamaria.andronic@dlapiper.com

Slovakia
Michaela Stessl
Partner
Corporate
+421 (0) 259 202 142
michaela.stessl@dlapiper.com

Slovenia
Jasna Zwitter-Tehovnik
Partner
Finance & Projects
+43 (0) 1531 78 1025
jasna.zwitter-tehovnik@dlapiper.com

Spain
Diego Ramos
Partner
Intellectual Property & Technology
+34 (0) 91 790 1658
diego.ramos@dlapiper.com

Sweden
Johan Sundberg
Partner
+46 (0) 8701 78 24
johan.sundberg@dlapiper.com

Switzerland
Roland Mathys
Partner
Information and Communication Technology
+41 (0) 44 215 3662
roland.mathys@swlegal.ch

UK
John Wilks
Partner
Intellectual Property & Technology
+44 (0) 20 7796 6288
john.wilks@dlapiper.com

APAC
Scott Thiel
Partner
Intellectual Property & Technology
+852 (0) 2103 0519
scott.thiel@dlapiper.com

US
Jim Halpert
Partner
Co-Chair, US Cybersecurity Practice
Co-Chair, Global Data Protection,
Privacy and Security Practice
+1 202 799 4441
jim.halpert@dlapiper.com

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

www.aon.com

About DLA Piper

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at **www.dlapiper.com**.

DLA PIPER

AON
Empower Results®