Gníomhaireacht Bainistíochta an Chisteáin Náisiúnta
National Treasury Management Agency

An Ghníomhaireacht um Éilimh ar an Stát
State Claims Agency

State Indemnity Guidance

SIG 09: Cyber and Data Breach Risks

a) Introduction

The purpose of this State Indemnity Guidance (SIG) is to assist Delegated State Authorities (DSAs)[1] to manage and mitigate the risks associated with cyber security and data breaches within their organisation. Cyber risk means any risk of financial loss or damage to the reputation of an organisation arising from a failure or breach of its information and communications technology (ICT).

A data risk means the unauthorised or illegal viewing, access or retrieval of information or data. Cyber and data risks are complex and continually evolving.

b) What cover does the GIS provide?

The General Indemnity Scheme (GIS)[2], as operated by the State Claims Agency (SCA), provides cover to DSAs for risks relating to personal injury and third party property damage arising from an act or omission of the DSA, which includes cyber or data risks.

c) What is Cyber and Data Breach Insurance?

Cyber and/or data breach insurance is triggered following a cyber-security or data breach incident. It will not prevent the occurrence or threat of an incident or breach occurring. However, cyber/data breach insurance may mitigate the risk and financial implications. *Table 1- Summary of Coverage for Cyber and Data Breaches* outlines the key covers provided by the GIS and potentially by commercial insurance where purchased.

d) Does my DSA need Cyber/Data Breach Insurance?

State guidance in relation to the purchase of Insurance is set out in Section C8 'International Agreements and Contingent Liabilities' of the 'Procedure and Practices in Government Accounting'. Self-insurance should be the primary choice, however purchasing cyber/data breach insurance may be a practical consideration if following risk assessment there is still a likely potential for a significant financial impact if an incident/breach were to occur and funding would be difficult to obtain.

Identifying loss scenarios (e.g. loss of intellectual property, breach of information, reputational loss etc.) and quantifying financial exposures may assist a DSA in determining the risk, control measures and the requirement for cyber/data breach insurance.

e) Do I need Cyber/Data Breach Insurance for the General Data Protection Regulation (GDPR)?

The GDPR sets out measures organisations must take to protect individual's personal data in line with modern privacy needs and concerns. DSAs must ensure that they comply with the GDPR, and consider existing systems and processes to achieve compliance. The decision to purchase insurance should be based on the risk as set out in part d) & f) of this guidance. It is worth noting that fines and penalties are unlikely to be insurable under a cyber-insurance policy.

[1] **Delegated State Authority (DSA) - R**efers to all bodies where management of personal injury and third-party property damage claims against the body is delegated to the SCA. This includes State Agencies, healthcare enterprises, community and comprehensive schools and prisons.

[2] **General Indemnity Scheme (GIS)** - Indemnity is a protection against possible damage or loss, typically a promise of payment should damage, or losses occur. The GIS, as operated by SCA, is given to State authorities by the State, to compensate third parties or individuals for any losses that incur as a result of the activities of the State (or State body), where the State has been negligent by act or omission.

Table 1: Summary of Coverage for Cyber and Data Breaches– guide only insurance policy cover will vary. Coverage Type	GIS	Cyber/ Data Breach Insurance	Professional Indemnity
Losses to your Organisation			
Business costs of a cyber/data breach Costs of restoring, recollecting or recreating data after a leak or breach Loss of revenue Support and notification costs	*No*	*Yes*	*No*
Fines and penalties for data breach	*No*	*No*	*No*
Losses to a Third Party			
Damage and costs of a cyber/data breach which was the result of an action on the part of your organisation E.g. through infringement performed through computer systems or the business websites or transmission of virus.	*Yes**	*Yes*	*Yes***
Liabilities of breach of privacy of confidentiality	*No*	*Yes*	*Yes*
Negligence claim for personal injury E.g. psychological injury which is the result of a cyber/data incident	*Yes*	*No*	*Yes*

*Covered only where there is a negligence claim taken by the third party for property damage.
** Professional indemnity policy will require a cyber/data breach.

f) What does my DSA need to do to manage Cyber/Data Breach Risks?

DSAs must have appropriate risk management systems in place to protect their ICT and data. DSAs must risk assess and implement controls to manage the risks. Examples of sources of a threat are included in Table 2 below:

Table 2: Sources of Cyber Risk Threats

	DELIBERATE	ACCIDENTAL
INTERNAL	• Access/manipulation of ICT by unauthorised internal user (e.g. disgruntled/rogue staff); • Release, destruction, corruption or theft of critical or confidential data; • Creation of false transactions.	• Transmission of computer virus or malicious content; • Operational error by employees; • Records or computing device lost; • Infringement on intellectual property rights.
EXTERNAL	• Access and manipulation of ICT by unauthorised external user, data release, destruction, corruption or theft of critical/confidential data; • Introduction of a computer virus, malware etc.; • Phishing or fraudulent practice; • Encryption of critical data.	• Operational error of third party impacting DSA's ICT; • Third party releases confidential data in their control; • Introduction of virus/malware/other by third party.

Table 2: Sources of Cyber Risk Threats

g) What liability limits for Cyber/Data Breach risks do I need for engaging a contractor?

Cyber/data breach risks should be considered when engaging a contractor who will have access to your ICT systems and/or who is processing information on your behalf. Please refer to "Guidance on Indemnity and Insurance SCA-GD-01" for more information.

Limits in relation to Cyber/Data breach Insurance should be applied according to the risk presented by the nature of the tender, the following is provided as a guide:

- *For low risk*: A €1 million limit of liability is typically recommended for low risk ICT projects, where there is limited or no interaction with confidential records, financial records, personal information, etc.;
- *For medium-high risk*: A €5 million limit of liability is typically recommended for medium to high risk ICT projects, where there is potential for the loss or exposure of confidential records, financial records, personal information, etc.

h) Should my DSA agree to Data Protection and GDPR indemnity clauses?

A DSA may require or be required to agree to an indemnity clause for GDPR as part of a contract for service or a data sharing agreement. These are appropriate; however as with any contract/agreement the SCA would advise:

- Reviewing the clauses carefully and seek DSA legal advice before signing;
- Ensure there are no hold harmless agreements included;
- Be familiar with the insurance/indemnity cover required on foot of these agreements.

i) Where can I get Additional Information

National Cyber Security Centre (NCSC)
General Data Protection Regulations, Data Protection Commissioner
Irish Data Protection Act 2018

j) When to contact the SCA?

The SCA are available to advise DSAs on insurance and indemnity queries.
Please email stateclaims@ntma.ie.