Data Protection Officers (China)

by **Amy Gong, Anjie Broad**

Practice notes | Law stated as of 01-May-2026 | Asia, China

A Practice Note that provides an overview of the role, responsibilities, and legal requirements for a data protection officer (DPO) under the legal framework of China. This Practice Note focuses on the Personal Information Protection Law 2021 (2021 PIPL) and clarifies when a personal information processor must designate a DPO, particularly when processing the data of more than one million individuals. It examines the DPO's positioning within an organisation's privacy management program, distinguishing the role from other leadership positions mandated by China's Cybersecurity Law and Data Security Law. Furthermore, this Practice Note discusses DPO qualifications, typical office structures, and essential considerations for internal reporting lines to maintain independence and avoid conflicts of interest. The DPO's statutory duties are explored in detail, covering compliance oversight, audit responsibilities, and their function as a key liaison with regulatory authorities and data subjects. Guidance is also provided on the 2021 PIPL's extraterritorial scope, which is critical for multinational organisations operating in the region.

China (PRC) has a vast and highly active internet user base, with digital services forming an integral part of daily life for individuals and businesses. This scale of digital activity generates vast quantities of data on a daily basis, much of which constitutes personal information (PI). As the digital economy continues to expand and AI develops rapidly, the asset value of data has become increasingly evident. At the same time, compliance and security risks associated with PI processing have become material issues that organisations can no longer treat as secondary considerations.

This Practice Note examines the role of the data protection officer (DPO) in the protection of PI under the legal framework of China. For terminology, it should be noted that the Personal Information Protection Law of the PRC 2021 (2021 PIPL) uses the term "person in charge of personal information protection." For ease of reference and comparison with international practice, this Note uses DPO to refer to that role, without intending to alter its legal meaning. Unless the context indicates otherwise, references in this Note to data are limited to PI.

This Note provides an overview of:

- When a DPO is required.
- The DPO's role and positioning within an organisation's privacy management program.
- Typical DPO office structures.
- The DPO's qualifications.
- The DPO' s duties and responsibilities in China.

Data Protection Regulation in China

Requirements for Appointing a DPO

The principal legislation governing PI protection in China is the 2021 PIPL, which provides a dedicated legal framework in an area where relevant requirements were previously dispersed across various civil and criminal laws or judicial interpretations. The 2021 PIPL sets out rules on personal information processing; cross-border transfers, individuals' rights, obligations of personal information processors, regulatory powers, and legal liability.

Where a PI processor processes PI in a volume reaching the threshold prescribed by the Cyberspace Administration of China (CAC), the 2021 PIPL requires it to designate a person in charge of PI protection, commonly referred to as a DPO, to

supervise its PI processing activities and the protective measures adopted. The PI processor must also publicly disclose that person's contact details and submit the individual's name and contact details to the competent authority performing PI protection duties. (Article 52, 2021 PIPL.)

For several years following the 2021 PIPL's implementation, the relevant volume threshold was not specified through a unified quantitative standard at the statutory level. In practice, some companies (particularly foreign-invested enterprises with more mature compliance frameworks) chose to establish a DPO or equivalent role by reference to national standards and industry practice.

Before the 2021 PIPL came into effect, the State Administration for Market Regulation (SAMR) and the Standardization Administration of China jointly issued the recommended national standard Information Security Technology – Personal Information Security Specification (GB/T 35273-2020) (2020 PIS Specification). Although not legally mandatory, the 2020 PIS Specification has long served as an important reference for corporate privacy compliance in China. It sets out advisory triggers for appointing a PI protection officer, including where the organisation meets any of the following conditions:

- Its core businesses involve PI processing, and it has more than 200 employees.
- It processes PI of more than one million individuals or expects to do so within the next 12 months.
- It processes sensitive PI of more than 100,000 individuals.

On 12 February 2025, the CAC issued the Measures on the Administration of Personal Information Protection Compliance Audits 2025, which require PI processors processing PI of more than one million individuals to designate a DPO to take charge of PI protection compliance auditing (Article 12).

Subsequently, on 18 July 2025, the CAC issued the Announcement on Implementing Information Reporting for Persons in Charge of Personal Information Protection 2025 (2025 Reporting Announcement), which sets out the following filing deadlines:

- Processors that reach the one-million-individual threshold on or after 18 July 2025 to complete the filing within 30 days of reaching the threshold.
- Processors that had already reached the threshold before 18 July 2025 were required to complete the filing by 29 August 2025.
- Where the filed information undergoes a substantive change, the processor must complete the amendment procedures within 30 working days from the date of the change.

Accordingly, the legal and regulatory framework has crystallised a relatively clear designation and filing threshold in practice. A processor that handles PI of more than one million individuals must designate a DPO (person in charge of PI protection) and complete the required filing within the applicable deadline.

DPO v Other Cybersecurity or Data Security Leaders: Conceptual Distinction

In addition to the DPO role under the PI protection regime, China's legal framework also imposes organisational requirements relating to cybersecurity and data security. For ease of reference, the key roles and structures are summarised below.

Cybersecurity Responsible Person

Under the Cybersecurity Law of the PRC 2025 (2025 CSL, with effect from 1 January 2026), network operators are required to:

- Establish internal security management systems and operating procedures in accordance with the multi-level protection scheme (MLPS). For more information, see Practice Note, Cybersecurity Risk Classification Under China's Multi-Level Protection Scheme.

Designate responsible personnel.

Implement cybersecurity protection obligations.

(Articles 23 and 36, 2025 CSL.)

The term network operator is broadly defined and generally covers network owners, managers, and network service providers (Article 78, 2025 CSL). In practice, entities that qualify as network operators typically should identify a cybersecurity lead within their governance structure, whether designated as Chief Security Officer (CSO), Chief Information Security Officer (CISO), or by another equivalent title.

Data Security Responsible Person and Data Security Management Office

The Data Security Law of the PRC 2021 (2021 DSL) requires processors of important data to designate a person responsible for data security and establish a data security management body to implement data security protection responsibilities (Article 27).

Important data is identified and managed through sectoral and regional catalogues developed by competent authorities under the data classification and grading system (Article 21, 2021 CSL).

Where an enterprise is determined to process important data, the compliance expectation is therefore not limited to appointing a responsible person, it also includes establishing an appropriate management structure to support higher-level governance requirements.

In addition, under the Regulations on Network Data Security Management 2024 (2024 Network Data Regulations, with effect from 1 January 2025), where a network data processor processes PI of more than 10 million individuals, it may be required to comply with governance requirements broadly aligned with those applicable to important data processors, including:

Designating a network data security responsible person.

Establishing a corresponding management body.

(Articles 28 and 30, 2024 Network Data Regulations.)

Accordingly, at very large scale, organisations may need to operate both:

A DPO function for PI protection compliance.

A data security function (data security responsible person and management body) to meet data security governance requirements.

Dedicated Security Management body for Critical Information Infrastructure (CII)

Where a network operator's facilities or systems are designated as critical information infrastructure (CII), the Regulations on Security Protection of Critical Information Infrastructure 2021 (2011 CII Regulations) require the operator to establish a dedicated security management body, and to conduct background checks for the responsible person and key personnel (Article 14). The dedicated body's responsibilities typically extend to the establishment and implementation of cybersecurity, data security, and PI protection systems (Article 15). As a result, CII operators generally will maintain both:

A DPO designation under the 2021 PIPL (where applicable).

A dedicated security management body for comprehensive security governance.

From an organisational governance perspective, the framework can be understood at a high level as follows (subject always to industry classification, whether important data is involved, and whether the entity is designated as CII):

Processing PI of fewer than one million individuals: generally, does not trigger the statutory designation or filing threshold for a DPO, but the organisation should still identify cybersecurity responsibilities under the 2025 CSL. If the

organisation processes important data or is designated as CII, additional data security or dedicated security body requirements may apply.

Processing PI of more than one million but fewer than ten million individuals: generally, requires designation and filing of a DPO (person in charge of PI protection). Cybersecurity responsibilities should also be defined under the 2025 CSL. If important data processing or CII designation applies, additional governance requirements will be triggered.

Processing PI of more than ten million individuals: in addition to the DPO function, enhanced network data security governance may apply (for example, designation of a network data security responsible person and a corresponding management body), while continuing to meet MLPS or cybersecurity governance requirements.

In practice, cybersecurity and data security leadership roles (often grouped under CSO, Data Security Officer (DSO), or CISO-type functions) typically require substantial technical and information security expertise, and organisations frequently consolidate these responsibilities within a single position or reporting line. However, these roles are not equivalent to the DPO function. Given the DPO's compliance oversight mandate and the need to avoid structural conflicts of interest, organisations should carefully assess whether cybersecurity or data security leadership roles can be combined with the DPO role in each governance model (See Forms of Data Protection Office in Organisations of Different Sizes).

Explanation of Several Key Concepts

Scope of Application for 2021 PIPL

The 2021 PIPL applies to the processing of PI of natural persons within China. The term natural person is not limited by nationality and includes both Chinese nationals and foreign individuals.

The 2021 PIPL also has extraterritorial reach. Where PI of individuals located in China is processed outside China, the 2021 PIPL applies if any of the following circumstances is met:

The processing is for the purpose of providing products or services to individuals located in China.

The processing is undertaken to analyse or assess the behavior of individuals located in China.

Other circumstances stipulated by laws or administrative regulations.

(Article 3(2), 2021 PIPL.)

In addition, where the 2021 PIPL applies to an overseas PI processor, the processor is required to establish a dedicated entity or appoint a representative within China to handle PI protection-related matters, and to file the relevant information (including the name and contact details of the entity or representative) with the competent authority (Article 53, 2021 PIPL). In practice, the filing approach may vary depending on corporate structure (for example, whether the overseas processor has an onshore presence or an affiliated entity), and should be assessed on a case-by-case basis.

Personal Information (PI)

PI means all kinds of information relating to an identified or identifiable natural person recorded by electronic or other means, excluding anonymised information (Article 4, 2021 PIPL). The key determinants are therefore:

Identifiability.

A link to a natural person.

This definition follows a similar core logic to the concept of personal data in the EU General Data Protection Regulation ((EU) 2016/679) (GDPR), as both focus on information relating to an identified or identifiable natural person. However, the differences remain in their scope and regulatory architecture. For more information, see Practice Note, Overview of EU General Data Protection Regulation: Personal Data and Data Subjects.

PI Processor

A PI processor refers to an organisation or individual that independently determines the purpose and means of processing PI (Article 73(1), 2021 PIPL). Unlike the GDPR's controller or processor distinction, the 2021 PIPL uses PI processor as the principal responsible entity. Functionally, the definition of a PI processor in the 2021 PIPL largely aligns with the GDPR concept of a controller.

Privacy Management Program

A relatively comprehensive privacy compliance management program typically comprises four pillars:

- Governance (organisational governance structure, internal management systems, and operating procedures).
- Lifecycle compliance controls.
- Security and technical measures.
- Continuous improvement.

Article 51(1) of the 2021 PIPL requires PI processors to establish internal management systems and operating procedures. In practice, this means an organisation should:

- Clearly allocate responsibilities and decision-making authority for PI protection.
- Establish appropriate communication and reporting lines, implement compliance review workflows (for example, for new products, vendor onboarding, and material changes to processing).
- Maintain accountability mechanisms to support a coherent governance framework.

Where a processor handles PI above the threshold prescribed by the CAC, Article 52 of the 2021 PIPL further requires the designation of a DPO. For organisations processing PI of more than one million individuals, the relevant implementing rules (including the compliance audit regime) effectively make the DPO designation expectation more concrete in practice. From a governance perspective, organisations should therefore embed the DPO's role, authority, reporting line, and accountability arrangements into their organisational structure and operating procedures, so that the DPO can effectively supervise PI processing activities and the protective measures adopted.

The recommended national standard Data Security Technology - Compliance Audit Requirements for Personal Information Protection (GB/T 46903-2025) (effective from 1 July 2026) (CARPIP-46903) provides a useful audit-oriented reference for implementing the DPO function. It highlights whether:

- The DPO's responsibilities are clearly defined, and whether the DPO is granted sufficient authority to coordinate relevant internal departments and personnel (Section 6.21.2).
- The DPO has the right to provide recommendations on major decisions relating to PI processing (Section 6.21.3).
- The DPO has the authority to stop non-compliant processing and require corrective measures (Section 6.21.4).

Although CARPIP-46903 is not legally binding, it is likely to be treated in practice as an important benchmark for compliance implementation and audit readiness. To avoid a paper DPO with an unclear mandate or limited ability to perform its duties, or conversely, role overreach and internal friction, organisations should integrate the DPO's mandate, operating mechanisms, and oversight processes into their governance framework in a way that is practicable and auditable.

Lifecycle Compliance Management for Personal Information

Lifecycle compliance management is central to the 2021 PIPL, covering the full range of processing activities, including collection, storage, use, processing, transmission, provision, disclosure, and deletion. Organisations engaging in this processing should implement controls to ensure compliance with key statutory obligations, such as:

- Appropriate notice and consent (where applicable).

Necessity and data minimisation.

Impact assessments.

Security measures.

Mechanisms for responding to data subject rights requests.

In this context, organisations should ensure that the DPO has:

Adequate visibility into PI processing activities.

Authority to conduct compliance review.

The ability to supervise remediation.

For specialised compliance tasks, such as PI protection impact assessments (PIAs) and cross-border data transfer compliance, the DPO may, pursuant to internal authorisation and governance arrangements, initiate workstreams independently or lead cross-functional coordination.

The 2021 PIPL also requires public disclosure of the DPO's contact details (Article 52), which in practice often positions the DPO (or the DPO office) as a key channel for handling data subject requests and external enquiries. In regulatory inspections, investigations, or incident response, the DPO likewise typically serves as a primary liaison between the organisation and the competent authorities.

Security and Technical Measures for Personal Information Protection

The 2021 PIPL requires organisations to implement classified and tiered management of PI and to adopt appropriate security measures, such as encryption and de-identification (Article 51). Common technical implementations include:

Data classification and labelling.

Access controls and authentication.

Encryption for storage and transmission.

Security scanning and penetration testing.

End-to-end traceability through logging and audit mechanisms.

These measures are ordinarily implemented by internal information security or technical teams. The DPO does not usually perform technical operations directly; however, the DPO should supervise whether the measures adopted are compliant, adequate, and effective. This includes assessing whether:

Anonymisation or de-identification measures satisfy applicable legal standards.

Access control aligns with risk-based management and least-privilege principles.

Vulnerabilities and security risks are identified and remediated in a timely manner.

Continuous Compliance Improvement

PI protection compliance is a dynamic, ongoing process that requires continuous optimisation in response to regulatory developments, evolving enforcement expectations, and changes to business models and processing activities. The DPO should lead (or oversee) regular training and awareness programs within the organisation, consistent with the DPO's statutory duties and internal mandate.

In accordance with the compliance audit regime, the DPO (as the responsible person for PI protection compliance auditing) is

expected to support periodic audits, gap identification, remediation tracking, and verification of corrective actions. By implementing a closed-loop mechanism that links training, regular audits, remediation, and iterative updates to policies and procedures, organisations can systematically enhance the maturity and effectiveness of their privacy compliance management program.

Data Protection Office Structure

Internal Reporting Lines and DPO's Independence

China's current legislation does not prescribe in detail to whom a DPO must report. However, given the DPO's supervisory mandate, the role should be positioned with sufficient independence to avoid undue influence from operational or revenue-generating functions.

The 2020 PIS Specification suggests that organisations should clearly designate the legal representative or principal responsible person as ultimately accountable for PI security, and that the DPO should participate in key decision-making and report directly to the organisation's top leadership (Section 11.1(a) and (b)).

Consistent with general corporate governance principles, where the board or the general manager typically determines internal governance structures and senior appointments, a prudent approach is to ensure that the DPO has a direct reporting line to the highest management level (for example, the principal responsible person, the general manager or CEO, or the board of directors or a board committee), or to a governance body duly authorised to make decisions on behalf of senior management. This helps preserve both the independence and effectiveness of the DPO's oversight function.

By way of cross-jurisdictional comparison, the GDPR requires the DPO to report directly to the highest management level of the controller or processor (Article 38(3)). While this requirement does not apply in China, its underlying governance rationale is instructive for multinational organisations designing reporting lines and escalation mechanisms.

Forms of Data Protection Office in Organisations of Different Sizes

For small and medium-sized organisations with limited data processing capacity, the single DPO model is typically adopted, where the DPO oversees PI protection and related regulatory framework development, while coordinating across departments to ensure the effective implementation of daily compliance practices.

For large internet platforms or enterprises handling massive data volumes, it is essential to establish both enterprise-level DPOs and business or system-level DPOs, supported by dedicated teams, to address compliance governance needs across multiple products, systems, and regions.

In practice, some organisations implement multi-layered compliance defenses alongside DPO roles to strengthen internal privacy governance. For example, a three-tiered defense system may be adopted:

- Business units from the first line through self-inspections and privacy-by-design governance.
- Professional data protection specialists from the second line by providing compliance support and developing governance mechanism.
- Internal audit functions from the third line by conducting independent audits and oversight.

Part-Time work and Conflict of Interest: Avoid Being both the Referee and the Player

The core role of a DPO is compliance oversight and coordination support. If the DPO also assumes key responsibilities for determining the purposes, methods, or implementation of security measures for personal data processing, structural conflicts of interest may arise. For instance, appointing a DSO or Security Department Head as the DPO could lead to oversight of the very data processing and security protocols they themselves oversee or approve, thereby compromising supervisory independence.

Unlike the GDPR, the 2021 PIPL does not explicitly list conflict of interest prohibitions. However, considering regulatory oversight roles and operational independence, organisations should avoid appointing a DPO to a position that may lead to

significant conflicts of interest. In cross-border regulatory practices, certain cases have explicitly identified safety roles concurrently serving as DPOs as a risk point for conflicts of interest, resulting in penalties or corrective measures (see Polish SA: administrative fine of EUR132 000 for improper positioning of the DPO and failure to include profiling in documentation).

External DPO or Group DPO: Feasibility and Compliance Risks

Under the GDPR framework, the DPO can be appointed from outside. The 2021 PIPL currently does not explicitly prohibit external personnel from serving as DPOs. However, organisations generally prefer natural persons within the organisation to assume this role in practice because:

- The 2021 PIPL employs the term PI protection officer, and the relevant contextual responsibilities suggest that, in practice, the role is more effectively performed by an identifiable individual who is embedded in, or has sufficient access to, the organisation's PI governance structure.
- A DPO is required to perform routine duties including ongoing supervision, cross-departmental coordination, incident response, and external communications.
- The information reporting mechanism for announcements and similar communications typically requires the submission of PI.

However, for large conglomerates, since member companies may share certain systems, there could be instances of DPOs holding concurrent roles across subsidiaries within the group. Current regulatory requirements for DPO reporting indicate no explicit guidance on permitting cross-company appointments. In practice, compliance assessments and feasibility evaluations must be conducted by aligning the group's organisational structure with regulatory mandates.

DPO Qualifications

The 2021 PIPL does not prescribe detailed qualification criteria for a DPO. In practice, the 2020 PIS Specification suggests that the DPO should be appointed from individuals with relevant management experience and professional knowledge in PI protection (Section 11.1(b)).

From an audit-readiness perspective, CARPIP-46903 similarly focuses on whether the DPO has the requisite professional experience and knowledge, including familiarity with PI protection laws and regulations, and proposes practical verification methods such as reviewing internal appointment documentation and checking the DPO's identity, background, and work experience (Section 6.21.1).

Accordingly, DPO qualifications can be summarised as two core competency areas:

- Professional competence. A DPO should have a solid command of the 2021 PIPL and relevant implementing rules, regulatory policies, and key compliance mechanisms, such as notice and consent (where applicable), PI protection impact assessments, cross-border data transfer compliance, data subject rights request handling, and incident response, and be able to translate legal requirements into workable internal policies, procedures, and controls.
- Governance and management capability. A DPO should also have the organisational and leadership skills needed to drive implementation, including cross-functional communication and coordination, remediation tracking and execution, designing and delivering training and awareness programs, and supporting periodic audits and closed-loop continuous improvement.

DPO Duties and Responsibilities

The 2021 PIPL expressly assigns the DPO a statutory oversight function in relation to PI processing activities and the protective measures adopted and requires public disclosure of the DPO's contact details, as well as filing with the competent authority (see Requirements for Appointing a DPO). The compliance audit regime further ties PI protection compliance auditing responsibilities to the DPO role. Together, these rules form the principal legal basis for the DPO's core duties under the current regulatory framework in China.

Before the 2021 PIPL came into force, the 2020 PIS Specification set out a list of DPO responsibilities (ten duties under Section 11.1(d)). Some of those formulations, however, do not fully align with the DPO's current positioning as an

independent compliance oversight function. For example, describing the DPO as the overall coordinator of internal PI security operations and the direct custodian of PI protection risks conflates the DPO function with the responsibilities of information security teams. To better align with the statutory framework and governance expectations, it is helpful to frame the DPO's role as:

A compliance overseer.

A cross-functional coordinator.

A professional compliance enabler.

A statutory external liaison.

The DPO's responsibilities can then be articulated as follows.

Statutory and Core Supervisory Responsibilities (Supervision and Auditing)

End-to-end compliance oversight. Supervise compliance across the full lifecycle of PI processing (including collection, storage, use, processing, transmission, provision, disclosure, and deletion); raise objections where non-compliant practices are identified and drive corrective actions to completion.

Compliance audit leadership or coordination. Lead or coordinate PI protection compliance auditing: formulate audit plans; organise audits (including leveraging internal audit resources or external professional support); review audit reports; track remediation to closure; and fulfil any reporting obligations under applicable audit rules (where triggered).

Implementation assurance for policies and procedures. Monitor implementation of privacy policies, internal rules, and operating procedures; identify gaps in execution and promote revision and continuous improvement.

Cross-functional coordination (governance mechanisms and collaborative delivery).

Coordination mechanisms. Establish and operate cross-departmental communication and coordination mechanisms across business, legal, product or tech, security, and HR functions, to support standardised and systematised implementation.

Major or special compliance matters. Coordinate major or specialised compliance workstreams (for example, new product or feature launches, data sharing arrangements, and the selection of cross-border data transfer compliance mechanisms), intervening at key decision points to review and provide compliance recommendations.

Professional Compliance Support (Operational Best Practices)

Regulatory interpretation and actionable guidance. Provide management and business teams with interpretations of laws and regulatory expectations, and translate them into practical, business-specific recommendations.

Training and effectiveness validation. Build a tiered training program (for example for management, business roles, or technical roles) and validate effectiveness through questionnaires, testing, or sampling checks.

Privacy by design. Participate early in project initiation, product design, and iteration to embed compliance and risk controls upstream, reducing post-launch remediation costs.

Third-party and contracting support. Review data protection clauses and processing arrangements in external collaborations (including entrusted processing, sharing, and transfers), and recommend clause enhancements and risk mitigation measures.

Regulatory Interface and Data Subject Engagement (External Communication and Incident Handling)

Regulatory liaison. Act as a key point of contact with competent authorities (including CAC and other relevant regulators), supporting inspections, investigations, and required filings or updates.

Data subject rights and complaints. Coordinate processes for handling data subject requests and complaints and review external-facing responses for legal and regulatory compliance.

Incident response participation. Participate throughout PI security incident response: assess legal risk, support notifications or communications with regulators and affected individuals where required, drive remediation, and establish post-incident review and improvement mechanisms.

Compliance System Built-out (Top-Level Governance Design and Documentation)

Institutional design. Within the scope of corporate authorisation, lead or participate in drafting and updating the organisation's PI protection governance documents (policies, procedures, templates, and operating rules) to ensure alignment with current law and regulatory expectations.

Compliance records and audit trail. Require relevant technology or security functions to provide compliance-critical documentation (for example, processing inventories, process flows, and security measures), and establish and maintain compliance archives to support oversight, auditing, and regulatory reporting.

To make the DPO role effective in practice, organisations should put in place supporting safeguards, including:

A direct reporting line to the statutory responsible person or board (or an authorised governance body), to preserve independence from business functions.

Sufficient authority and access, including access to processing documentation, cross-functional coordination rights, the ability to raise compliance objections, and the ability to provide recommendations on material decisions.

Resourcing and budget, enabling the DPO to draw on internal compliance resources and, where appropriate, external advisers (for example, legal counsel and audit firms), while maintaining focus on oversight and coordination rather than day-to-day operational execution.

Duties of Others in the Data Protection Office

Effective implementation of an organisation's PI protection program depends on coordinated execution across business, product and engineering, information security, technology, and legal functions for example, each operating within its statutory obligations and internal mandate. In this governance model, the information security function is typically the key enabling capability for protecting PI (in particular, through technical controls, monitoring, and incident response).

For organisations processing PI at very large scale (for example, more than ten million individuals), regulatory requirements may also necessitate establishing a dedicated network data security management function (for example, a network data security management body). This function's core responsibilities typically include:

Policies, procedures, and incident preparedness. Developing and implementing network data security management systems, operating procedures, and security incident emergency response plans.

Ongoing risk management and training. Regularly conducting risk monitoring and assessments, organising emergency drills, and carrying out education and training to enable timely identification and handling of network data security risks and incidents.

Handling complaints and reports. Receiving and processing complaints and reports relating to network data security.

(Network Data Regulations, Article 30.)

In addition, the DSO (or the equivalent network data security responsible person) responsible for network data security, often including the protection of PI, commonly serves as a key counterpart to the DPO in day-to-day governance. The role typically requires:

Specialised expertise in network or data security.

Relevant management experience.

Sufficient organisational authority, resources, and escalation or reporting capability to support implementation of data

security governance requirements and to coordinate effectively with the DPO function.

	END OF DOCUMENT	