Data Protection Office
Oversight and Regulatory Action Framework

Data Protection Office
Qatar Financial Centre

Qatar Financial Centre Authority ● PO Box 23245 ● Doha, Qatar
T: +974 4496 7777 ● F: +974 4496 7676 ● info@qfc.qa ● qfc.qa

Table of contents

Qatar Financial Centre Authority ● PO Box 23245 ● Doha, Qatar
T: +974 4496 7777 ● F: +974 4496 7676 ● info@qfc.qa ● qfc.qa

Introduction

The QFC Data Protection Oversight and Regulatory Action Framework sets out the Data Protection Office's (the "DPO") approach to oversight of and regulatory action against firms that have breached the provisions of the QFC Data Protection Regulations (the "Regulations") and Rules (the "Rules") 2021. Terms not otherwise defined in this Framework have the meaning given in the Regulations and Rules.

The Framework is designed to help create an environment within which Data Subjects are protected, while ensuring that businesses can operate efficiently and effectively.

The DPO will take what actions it deems necessary when ensuring compliance with the Regulations and Rules, whilst remaining mindful that the goal is not to restrict businesses with unnecessary or disproportionate use of financial penalties and other powers at its disposal.

This Framework sets out a risk-based approach to oversight and regulatory action, focusing on areas that will have the best outcomes for Data Subjects and the areas that could do the most harm when not complied with by firms. When considering what actions are appropriate, the DPO will consider the following:

- The severity of the breach;
- The impact of the breach on Data Subjects;
- The willingness of the organisation to cooperate with the DPO; and
- The organisation's history of compliance.

The DPO will work with other authorities, both local and international, where it is appropriate and where joint application of activity can achieve the best result and protection.

Framework objectives

This Framework sets out how the DPO will use its powers to protect Data Subjects' rights and legitimate interests when their Personal Data is Processed. The Framework aims to be fair, proportionate, and timely, and will assist the DPO in ensuring that its oversight and regulatory action activities are targeted, effective, and in line with the Regulations and Rules and its strategic objectives and plans.

In addition to setting out the DPO's oversight and regulatory action activities, as outlined in the Regulations and in Part 5 (Compliance and Enforcement Rules) of the Qatar Financial Centre Authority Rules ("QFCA Rules"), the Framework also provides guidance on how the DPO will handle privileged communications and how it will calculate the amount of a penalty for breaches of the Regulations.

When considering whether to take action, and in carrying it out, the DPO will seek to meet the following five objectives:

- Respond swiftly and effectively to breaches of the Regulations and Rules which fall within the DPO's remit, focussing on (i) those involving Sensitive Personal Data, (ii) those adversely affecting large groups of Data Subjects, and/or (iii) those impacting vulnerable Data Subjects.

- Use the supervisory powers of the DPO in a proportionate and consistent way focusing on those firms who are suspected of wilful or negligent misconduct and where Data Subjects rights and legitimate interests are most at risk.
- Promote legal compliance in accordance with the Regulations through fostering good practice and providing targeted guidance and interpretations on how to comply with all areas of the Regulations.
- To be proactive in identifying and mitigating new or emerging risks arising from technological and societal change.
- Working locally and internationally with other regulators to ensure the safe and compliant flow of data which benefits the economy and society.

The DPO will seek to meet these objectives by exercising its regulatory powers in the following ways:

- the DPO will take action proportionately and will exercise discretion as to when, in what manner, and to what extent regulatory action is required;
- in exercising this discretion, the DPO will consider the circumstances and context of each case
- the DPO will apply its resources to the areas of greatest risk and potential or actual harm to the community;
- the DPO will apply financial penalties and other enforcement powers where they are effective, proportionate and dissuasive to both the individual or organisation receiving the fine and more generally to those Processing Personal Data; and
- the DPO will seek to manage risks by sharing information effectively.

Legislative basis and scope

The DPO is empowered to take various regulatory actions for breaches of the following regulations:

- Data Protection Regulations 2021 (”Regulations”);
- Data Protection Rules 2021 (“Rules”).

The DPO is also empowered under the Regulations to use the provisions of the QFCA Rules, Part 5 Compliance and Enforcement Rules (“CER”), when enforcing provisions of the Regulations and Rules.

Guidance and support

While regulatory action remains crucial in enforcing compliance, the DPO recognises the significance of proactive guidance and support to foster a culture of compliance within organisations, promoting a collaborative approach between the DPO and firms. In order to assist firms, the DPO offers the following resources and support:

- Comprehensive guidance documents: The DPO develops comprehensive guidance documents that explain the requirements of the Regulations and offer practical advice on compliance, which are published by the QFCA.

- Tools and resources: The DPO provides various tools and resources on its website, including templates, checklists, interpretations, and best practice guidelines, to support firms in their compliance efforts.
- Communication channels: The DPO is accessible through multiple communication channels, such as email, telephone calls, and in-person meetings, to address inquiries, provide clarifications, and offer guidance on data protection matters.
- Education and outreach: The DPO conducts educational initiatives, such as presentations, conferences, and advice sessions, to raise awareness about data protection rights and obligations.

Evaluation and next steps

The DPO will keep this Framework under review and evaluate it regularly. The DPO will update it to reflect any amendments to the Regulations and/or Rules.

Qatar Financial Centre Authority ● PO Box 23245 ● Doha, Qatar
T: +974 4496 7777 ● F: +974 4496 7676 ● info@qfc.qa ● qfc.qa

A tiered approach to oversight and regulatory action

The DPO recognises the importance of a tiered approach to oversight and regulatory action in effectively enforcing the Regulations and Rules. This approach ensures that regulatory actions are commensurate with the seriousness of the breaches committed, thereby promoting fairness, proportionality, and accountability. By doing so, the DPO can allocate its resources efficiently, prioritise high-risk cases, and tailor enforcement actions to address the varying degrees of non-compliance.

For breaches where the violations are minor, unintentional, or result from inadequate procedures or systems and there is no direct or indirect harm to Data Subjects, the DPO will prioritise education, guidance, and support to foster compliance. This may include providing best practice recommendations, conducting awareness campaigns, or offering training sessions to the responsible firms. The emphasis will be on helping firms understand their obligations and take corrective measures to prevent future breaches.

For breaches involving intentional misconduct, harm or significant harm to Data Subjects, or repeated offences despite prior warnings or corrective actions, the DPO will employ stronger enforcement actions. These may include imposing enforcement notices or financial penalties commensurate to the severity of the violation. The DPO may also require mandatory audits or corrective action plans, and in extreme cases, collaborate with law enforcement agencies for criminal investigations. These measures aim to deter non-compliance, protect Data Subjects' rights and legitimate interests, and ensure a strong deterrent effect against the most egregious violations of the Regulations.

The DPO will take into consideration self-reporting, active engagement in issue resolution, and the presence of robust data protection systems and controls as factors that will be considered when determining its response.

By implementing a tiered model of oversight, the DPO can maintain a balanced and effective approach that ensures that any sanctions or disciplinary action are commensurate with the gravity of the breaches committed. This approach fosters compliance, encourages continuous improvement in data protection practices, and safeguards Data Subjects' privacy rights in an increasingly data-driven world.

Transparency

The DPO will make efforts to publish information about the volume and types of cases pursued, as well as the outcomes achieved, when deemed appropriate. This can encompass various actions such as thematic review results, corrective measures following an audit, enforcement notices, and financial penalties. Additionally, case study examples may be provided to demonstrate good practices or lessons learned.

To ensure confidentiality and sensitivity, if the DPO includes information derived directly from a thematic review, data protection audit or investigation, all necessary steps will be taken to redact and remove any potentially confidential or sensitive details from these examples.

Collaboration with international bodies and memoranda of understanding

The DPO recognises the importance of collaboration with international bodies in promoting effective enforcement of the Regulations. The DPO actively engages with organisations such as the Global Privacy Assembly (GPA) and the Global Privacy Enforcement Network (GPEN) to foster cooperation, exchange best practices, and harmonise enforcement efforts on a global scale.

Through membership of these bodies, the DPO contributes to shaping global data protection standards and guidelines. By participating in working groups and sharing experiences with other member authorities, the DPO can stay at the forefront of emerging trends and regulatory developments, enabling the DPO to enhance its expertise and ensure a consistent approach to enforcing the Regulations in alignment with international best practices.

The DPO recognises the importance of establishing strong collaborative relationships with both local and international bodies to facilitate information sharing and cooperation in enforcement actions. To this end, the DPO my enter into Memoranda of Understanding (MOUs) with various entities, including domestic regulatory agencies and international counterparts.

Regulatory activities

There are a number of important elements that work together to help the DPO oversee compliance and uphold the principles and requirement of the Regulations when dealing with firms. These include thematic reviews, data protection audits, investigations, and enforcement.

Own initiative reviews

Thematic reviews

The DPO conducts regular thematic reviews, focusing on specific aspects and requirements of the Regulations. Firms receive notices requesting their cooperation in the review of designated thematic area(s). The purpose of a thematic review is to identify trends and emerging risks, assess compliance with regulatory requirements, drive industry-wide improvement, enhance regulation and supervision, and ultimately protect Data Subjects and other stakeholders.

During the course of a thematic review the DPO will:

- ensure that the chosen thematic area aligns with the Regulations and Rules and to any supervisory priorities issued by the DPO from time to time.
- define the scope of the thematic review, specifying the extent and depth of the review required to evaluate compliance effectively.
- evaluate the adequacy and effectiveness of existing controls, such as data privacy notices, records of processing, data protection policies, privacy impact assessments, and incident response procedures, within the thematic area.
- assess the level of risk associated with identified compliance gaps, considering the potential impact on Data Subjects and the likelihood of harm or distress.
- determine appropriate actions to address non-compliance based on the severity of the issues discovered, aiming for proportionate and effective measures.

In addition, the DPO may:

- request the Data Controller or Data Processor to provide relevant documentation, policies, procedures, and records related to the thematic area under review.
- conduct interviews with key personnel involved in Personal Data Processing activities to gain insights into compliance practices and identify potential areas of improvement.
- require access to relevant systems, databases, and other technological infrastructure to assess data handling processes and safeguards.
- establish follow-up mechanisms to monitor the implementation of recommended measures and verify ongoing compliance with the thematic area's requirements.

The outcomes of a thematic review will be communicated to all firms on a no-names basis. This approach fosters industry-wide learning and improvement rather than singling out specific firms for criticism or punishment. The sharing of thematic review outcomes allows firms to gain insights into emerging risks, regulatory expectations, and best practices. It provides them with an opportunity to benchmark their own performance against industry standards and make necessary adjustments to their operations, policies, and procedures

When individual firms are found to fall short of the required standards in a thematic review, the DPO will typically work closely with those firms to address the identified deficiencies. The DPO's role is focused on collaboration and assisting firms in achieving compliance.

Data protection audits

The Regulations grant the DPO the power to undertake investigations and data protection audits. A data protection audit notice is issued by the DPO to a Data Controller or Data Processor to allow it to check whether the Data Controller or Data Processor is compliant with the Regulations. The notice may, for example, require the Data Controller or Data Processor to give the DPO access to premises and specified documentation and equipment.

The DPO may serve such a notice advising of its intention to review compliance with the Regulations at its discretion and on its own initiative at any time. The DPO will consider what action is suitable and proportionate, taking into account as the following non-exhaustive factors:

- The DPO's risk assessment or other regulatory action indicating a probability of non-compliance with the Regulations and Rules, coupled with a likelihood of harm or distress to Data Subjects.
- The need to verify compliance with a thematic review or with an enforcement notice.
- Communications or information (such as complaints, news reports, regulatory reporting, or publications) suggesting that the Data Controller or Data Processor is not Processing Personal Data in accordance with the Regulations and Rules.
- Non-response by the Data Controller or Data Processor to a notice of thematic review within a reasonable timeframe.

When assessing the risks associated with non-compliance with the Regulations, the DPO will take into account the factors that warrant the data protection audit, such as those above. Additionally, the DPO will consider other pertinent information, including reports from whistle-blowers and any data privacy impact assessments that have been conducted.

When determining the timeframe for compliance with a data protection audit notice the DPO will consider the most suitable and proportionate course of action. This data protection audit will take into account various criteria, including:

- The urgency in preventing or limiting serious harm to Data Subjects or intrusion into their privacy.
- The urgency in preventing the tampering, alteration, destruction, concealment, blocking, falsification, or removal of relevant evidence.
- Its scope, including the nature and extent of the request made to the firm.
- The additional burden placed on the firm when complying with an urgent, no-notice, or short-notice audit notice.
- The comparative effectiveness of alternative investigatory powers available to the DPO.

Investigations

The purpose of an investigation is to examine and assess the practices and operations of a Data Controller or Data Processor by reference to a particular matter. A notice of investigation serves as a formal notice to a Data Controller or Data Processor, informing them that an investigation is

underway. It requires them to provide the DPO with information, within a specified time frame, to assist with that investigation. Non-response or non-engagement by the Data Controller or Data Processor to such notice can lead to enforcement action, which may include the imposition of a financial penalty.

A notice of investigation is typically issued at the start of on an investigation but there may be circumstance in which the issuing of such a notice could jeopardise or otherwise frustrate the investigation. Therefore, the DPO reserves the right to not formally issues such notices where it deems appropriate.

When deciding to issue a formal notice of investigation, the DPO will consider:

- the risk of harm to Data Subjects posed by the Personal Data Breach, complaint or Processing under investigation;
- the need for formal responses within a defined time period; and
- the need to test responses, as it is a breach of the Regulations to give the DPO information that is false or misleading[1].

A notice of investigation may be accompanied with an order to halt Processing, to retain documents, or other such measures as the DPO considers fit depending on the circumstances surrounding the investigation.

When determining the period for compliance with notice of investigations, particularly when considering whether to issue an urgent notice of investigation, the DPO will have regard to what action is appropriate and proportionate, taking into consideration criteria such as:

- The nature and severity of the alleged violation or incident being investigated;
- The potential impact on Data Subjects' rights and freedoms;
- The urgency or time-sensitive nature of the investigation;
- The likelihood of data loss, unauthorised access, or further harm if Processing is not halted;
- The potential risk of evidence destruction or tampering if documents are not retained;
- The necessity to ensure compliance with the Regulations;
- The potential consequences for the firm if non-compliance is established;
- The need to protect Data Subjects' privacy and data security during the investigation;
- The resources and capabilities available to the firm for handling the investigation;
- The principles of fairness, transparency, and accountability in conducting the investigation.

Where a firm receives a notice of investigation and fails to provide a full response within the designated timeframe, regardless of whether the notice was urgent or not, the DPO may consider what action to take in response, taking into consideration various factors, including:

- The reasons behind the firm's non-compliance with the notice of investigation.

[1] QFC Authority Rules, Part 5 Compliance and Enforcement Rules, Rule 3.9 Obstruction of the QFCA

- Any commitments made by the firm regarding their intention to respond to the notice of investigation.
- The possibility of obtaining the requested information from an alternative source.
- The comparative effectiveness of alternative investigatory and enforcement powers available to the DPO. For instance, if the DPO determines that sufficient evidence exists to proceed with an enforcement action regardless of the response to the notice of investigation.
- The consideration of the public interest in determining the appropriate course of action.
- The DPO will also consider whether or not to issue a financial penalty notice (see below).

Essential elements of thematic reviews, data protection audits, and investigations

Inspecting and examining information and documents are critical components of all reviews and enable the DPO to gather objective evidence of compliance and assess the implementation of policies and procedures.

During these reviews, various forms of Personal Data, along with their associated logs and audit trails, are examined. This includes data stored in both manual and electronic formats, encompassing central, local, mobile devices, and media storage.

Through these reviews, the DPO evaluates how a firm:

- Collects, stores, uses, organises, adapts, or modifies Personal Data.
- Ensures the data or service it provides maintains confidentiality, integrity, and availability.
- Retrieves, consults, or utilises the information and Personal Data.
- Discloses Personal Data through transmission, dissemination, or other means of making it available.
- Implements processes for the proper retention and disposal of Personal Data.

The review and evaluation can be conducted on-site, either through discussions with staff to observe their practices or independently through sampling. This allows for a comprehensive understanding of the Data Controller's Personal Data Processing procedures.

In cases where electronic data is involved, the DPO may request manual copies or direct access to the systems to thoroughly assess the information. This facilitates a detailed examination of the Data Controller's data management practices.

It's important to note that any direct access to data would be limited to the identified records, conducted locally, and for a predetermined and agreed-upon time period. This ensures the appropriate and controlled handling of the data during the review process.

Data reviewed during the review, but not specifically identified in the initial notice, will only be taken off the Data Controller's site with their explicit permission. This ensures compliance with data protection and confidentiality requirements.

Assessment of documents

The DPO can ask for access to certain documents and information that explain how the firm manages and controls its operations, this includes for example:

- Plans & strategies;
- Policies;
- Procedures;
- Guidance;
- Training material;
- Supplier and employee contracts;
- Privacy statements;
- Privacy impact assessments;
- Job descriptions.

The DPO may also need access to specific Personal Data or classes of Personal Data, and to evidence that it is being handled in compliance with the policies and procedures which in turn ensure compliance with the Regulations. The level of access will only be enough to assess compliance.

The DPO may require access to information except for cases where:

- Legal professional privilege applies;
- The information possesses a significant level of commercial sensitivity;
- The information is exempt due to State national security or related laws.

The DPO acknowledges that there may be valid concerns regarding information that pertains to national security, international relations, or sensitive activities. In such cases, it is generally possible to conduct a data protection thematic review, data protection audit or investigation without accessing this information. However, when necessary and appropriate, the DPO will ensure that suitably vetted staff members inspect such information. Access will be limited to what is essential for the activity.

Firms can contact the DPO and request limitations on access to such information if a notice requires its disclosure. They can specify the minimum necessary access required to adequately evaluate their compliance with the Regulations. These requests must be submitted within 21 days of receiving the notice, unless the review is scheduled on shorter notice, in which case the request should be made as soon as reasonably possible.

In instances where the DPO needs to review Sensitive Personal Data, the confidentiality of this data will be respected. The DPO will restrict access to the minimum extent necessary for a thorough compliance assessment. The content of these records will not be taken off-site, copied, transcribed into working notes, or included in any reports by the DPO.

Interviews carried out during thematic reviews, data protection audits, and investigations

The DPO may conduct interviews to gain a deeper understanding of working practices and of how regulatory obligations are met. Interviews are held with departmental managers, operational staff, support staff (e.g., IT and security staff), and those involved in information and information governance.

Interviews involve discussions with:

- Staff and contractors;

- Staff of any Data Processors;
- Staff of relevant service providers mentioned in the relevant notice.

Whenever possible, the DPO schedules and agrees on interviews with the Data Controller or Data Processor prior to the on-site visit. A schedule of areas to be covered is provided, and the level and grade of staff to be interviewed (e.g., managers, operational staff) are discussed and agreed upon. Participants should be informed by the firm in advance of their expected involvement.

During interviews, the DPO uses questions to understand individual roles, processes related to handling Personal Data, and data security practices. The focus may include training and awareness, but the questions are not designed as tests or to catch individuals off guard.

Interviews may take place at individuals' desks or in separate rooms depending on circumstances and the need to observe the working environment or examine information and records. Typically, interviews are conducted on a one-to-one basis, although group interviews may be appropriate in cases where responsibilities are shared. Notes are taken by the DPO during the interviews.

While it is not necessary for interviewees to be accompanied by third parties, the DPO will accommodate reasonable requests for such accompaniment.

Efforts are made to limit interviews to staff identified in the agreed schedule. However, if it becomes evident during a thematic review, data protection audit, or investigation that access to additional staff is necessary, arrangements will be made with the consent of the Data Controller. Interviews with consenting third parties may also be conducted, for example, when they are present during desk-side discussions.

Interviews serve the purpose of assessing compliance and do not form part of any individual disciplinary investigation.

Individuals' names may be used in distribution lists and acknowledgments sections of reports, but they will not be referenced within the main body of any report. Job titles may be used when relevant.

Privileged communications

The DPO does not seek access to information protected by legal professional privilege. In the event that privileged information is inadvertently received by the DPO, strict confidentiality and sensitivity measures will be followed.

Non-engagement by firms in thematic reviews and data protection audits

Where a firm receives a notice of thematic review or data protection audit and does not fully respond within the applicable time period, whether urgent or not, the Commissioner will promptly apply for a court order requiring a response. The Commissioner may decide not to make such application, having regard to criteria including:

- the reasons for non-compliance with the relevant notice;
- any commitments given by the firm when responding to the relevant notice;
- whether the information has been or is likely to be obtained from another source;

- the comparative effectiveness of other investigatory and enforcement powers of the DPO. For example, the DPO may decide it has sufficient evidence to move to an enforcement action in any event; and
- the public interest.

If a Data Controller or Data Processor fails to engage with the DPO, the Commissioner will consider whether or not to issue a financial penalty notice.

Enforcement

The DPO has a number of enforcement powers to ensure compliance with the Regulations and Rules, and safeguard Data Subjects' rights and legitimate interests, including:

- Issuing warnings;
- Issuing reprimands;
- Issuing financial penalties; and
- Issuing enforcement notices

Selecting the appropriate regulatory activity for breaches of the Regulations

When determining whether and how to respond to breaches of the Regulations, the DPO may consider the following non-exhaustive factors:

- the nature and seriousness of the breach or potential breach;
- the duration of a breach or potential breach;
- where relevant, the categories of Personal Data affected (including whether any Sensitive Personal Data is involved);
- the number of Data Subjects affected or at risk;
- the extent of any exposure to physical, financial or psychological harm;
- whether the issue raises new or pre-existing issues;
- any concerns that technological security measures are sufficient to protect the Personal Data;
- the cost of measures to mitigate any risk, issue or harm;
- the public interest in regulatory action being taken (for example, to provide an effective deterrent against future breaches or clarify or test an issue in dispute); and
- whether another regulator, law enforcement body or competent authority is already taking (or has already taken) action in respect of the same matter.

Notice of intent

Except for cases involving warnings, and at the discretion of the Commissioner, the DPO will inform the firm of its intention to take an enforcement action by issuing a notice of intent (NOI). The NOI will present the findings of the investigation, detail the breach, outline any necessary actions required by the firm, and, if applicable, specify the recommended enforcement action along with the underlying reasons for the measure. In such situations, the firm will be granted a minimum of 21 calendar days to provide their responses regarding the matters addressed in the NOI.

Warnings

In cases where areas of non-compliance with the Regulations are identified but do not necessitate immediate enforcement action, the Commissioner can issue a warning to the firm, as a proactive approach. These warnings are designed to function as formal notices, communicating to firms the specific areas of concern that have been detected, and may highlight a set of corrective measures that are required to bring matter back into compliance with the Regulations.

Reprimands

In cases of serious or repeated non-compliance, the DPO may issue reprimands to firms. Reprimands are formal statements expressing the DPO's disapproval of the firm's actions or practices. Reprimands offer firms an opportunity to improve their data protection practices and overall compliance with the Regulations. They typically include a set of immediate and long-term corrective measures that firms are required to implement to regain compliance. The goal of a reprimand is to underscore the DPO's disapproval of the firm's actions and to act as a catalyst for change within the organisation, fostering a culture of data protection and compliance.

Financial penalties

When issuing a financial penalty, the DPO's objective is to ensure compliance with the Regulations and safeguard the rights and legitimate interests of Data Subjects. Financial penalties serve as both a suitable sanction for breaches of the Regulations and an effective deterrent.

The decision to impose a financial penalty and determine its amount is based on consideration of the following factors:

- The nature, seriousness, and duration of the failure;
- The intentional or negligent nature of the failure;
- Actions taken by the Data Controller or Data Processor to mitigate the impact on affected Data Subjects;
- The level of responsibility demonstrated by the Data Controller or Data Processor, including their implementation of technical and organisational measures in line with the Regulations;
- Any prior failures by the Data Controller or Data Processor;
- The degree of cooperation with the Commissioner to address and mitigate the risks associated with the failure;
- The types of Personal Data affected by the failure;
- How the infringement came to the attention of the Commissioner, including whether the Data Controller or Data Processor reported the failure and to what extent;
- Compliance with previous enforcement notices or financial penalty notices;
- Adherence to approved codes of conduct or certification mechanisms;
- Any other relevant aggravating or mitigating factors, such as financial gains or losses resulting from the failure;
- The effectiveness, proportionality, and dissuasiveness of the proposed financial penalty.

When a financial penalty notice will be appropriate

In most instances, the DPO will exercise its powers in cases of utmost severity, where there are significant violations of the Regulations and to the rights and legitimate interests of Data Subjects. Such cases typically involve intentional, deliberate, or negligent actions, or repeated breaches that result in harm or damage to Data Subjects. When assessing the level of harm or damage, the DPO may acknowledge that although the impact on each individual may be relatively minor, the cumulative effect on a large number of Data Subjects can be substantial, warranting the imposition of financial penalties.

Each case will be assessed based on its individual circumstances, however, the likelihood of a financial penalty being imposed is increased where there is:

- a high number of Data Subject effected;
- presence of damage or harm including potential distress or embarrassment;
- Involvement of sensitive Personal Data;
- Non-compliance with a notice of thematic review, audit, investigation, or enforcement notice;
- Repeated breach of obligations or failure to address previously identified issues or follow recommendations;
- Wilful action or inaction on the part of the firm;
- Insufficient implementation of reasonable measures, including privacy by design, to mitigate or prevent breaches;
- Failure to uphold the accountability provisions outlined in the Regulations.

Calculation of financial penalties

When setting the amount of a financial penalty the DPO will consider the following elements when setting the amount:

- a component that eliminates any financial benefit derived from the breach.
- a provision based on the magnitude and seriousness of the Personal Data Breach, considering the factors outlined in Article 36(2) of the Regulations.
- an element to account for any aggravating factors, such as:
    - the impact to vulnerable Data Subjects or children.
    - the breach resulting from deliberate actions aimed at personal or financial gain.
    - advice, interpretations, guidance, recommendations, or warnings, including those provided by the DPO, that have been disregarded or neglected.
    - where the privacy of a Data Subject has been significantly violated.
    - there is a failure to cooperate with the investigation or comply with an enforcement notice.
    - the firm having a history of repeated non-compliance with the Regulations.
- an amount to serve as a deterrent to others.
- a reduced amount or percentage (excluding the initial component) to account for any mitigating factors, including the ability to pay (financial hardship).

When dealing with instances of non-compliance with data security obligations, the DPO may assess the breach independently from the failure or delay to reporting. However, for all other

cases, the DPO will take a comprehensive approach by considering the entirety of the case when determining the level of financial penalty.

The DPO will issue a written confirmation of the financial penalty notice once all representations have been assessed and affected subjects will be informed of their rights to appeal.

Enforcement notices

The DPO may issue enforcement notices to firms, specifying actions they must take to achieve compliance within a given timeframe. Failure to comply with an enforcement notice may lead to further enforcement actions. The enforcement orders include orders to:

- erase Personal Data: orders requiring firms to delete or erase Personal Data under certain circumstances.
- fulfil Data Subject rights requests: orders to ensure firms fulfil Data Subject rights requests, such as requests for access, rectification, or deletion of Personal Data.
- inform Data Subject of Personal Data Breaches: orders to firms to inform affected Data Subject of any Personal Data Breaches that have occurred.
- cease or stop specific Processing operations: orders to halt or discontinue specific Processing operations that are non-compliant with data protection laws.
- stop data transfers to Recipients outside the jurisdiction: orders to cease or restrict the transfer of Personal Data to Recipients located outside the jurisdiction, where such transfers are deemed non-compliant.
- undertake a data protection impact assessment: orders requiring firms to conduct and provide evidence of a data protection impact assessment for certain Processing activities

An enforcement notice may be issued in the circumstances set out in Article 33(2) of the Regulations or Part 5 of the QFCA Rules.

An enforcement notice ensures compliance with the Regulations by mandating necessary actions or halting specific activities. Failure to comply with an enforcement notice may lead to further actions, including the potential imposition of a financial penalty. Such notices are typically issued to require specific corrective or preventive measures, such as:

- Repeated failure to fulfil Data Subject rights obligations or meet specified timelines (e.g., consistently delayed subject access requests).
- Non-compliance or potential non-compliance with the Regulations regarding the Processing or transfer of information to a third country.
- The necessity for the DPO to mandate communication of a Personal Data Breach to affected Data Subjects.

The notice will provide the following information and will be taken into account by the DPO when deciding to issue an enforcement notice:

- The responsible party and the rationale behind their obligation to take action.
- The details of the specific action to be taken.
- The procedure for reporting the completion of the action.
- The specified timeframe within which the action must be taken.
- The available process for initiating an appeal or challenge.

The timeframes specified in an enforcement notice are typically determined based on various factors, including the urgency of addressing non-compliance, the severity and extent of the violations, and the feasibility of implementing corrective actions or technology within specific lead times. These considerations aim to ensure that necessary actions are taken promptly and effectively. This evaluation will also consider the following criteria:

- the need to prevent or limit and risk of harm or loss of privacy to Data Subjects. For example, requesting a Data Controller stops using Personal Data for a specific purpose or takes action to protect Personal Data from security breaches;
- the extent of the enforcement notice's scope;
- the additional burden or impact on the firm when complying with an urgent enforcement notice within the specified timeframe; and
- the relative effectiveness of alternative enforcement powers available to the DPO.

Non-Compliance with enforcement actions of the DPO

If warnings, reprimands or enforcement notices issued by the DPO are not heeded, and the firm fails to take the appropriate action and corrective measures within the specified timeframe, further enforcement actions may be initiated, up to and including the issues of a financial penalty.

If the DPO considers that a firm has failed to comply with an enforcement notice or failed to pay a financial penalty within a stipulated timeframe, it may apply to the Civil and Commercial Court for an order directing the firm to comply with such notice and/or pay any outstanding financial penalties.

Publication

The DPO is committed to maintaining a transparent and responsible approach to regulatory oversight. As such, the DPO position is that, whenever deemed appropriate by the Commissioner and in accordance with relevant regulations and rules, decisions reached by the DPO will be made public. While certain sensitive, confidential, or proprietary information will remain protected, the DPO aims to provide concise and accessible summaries of its decisions to the public. By doing so, the DPO fosters an informed dialogue, facilitates understanding of the Regulations and what is expected of firms, and ensures a balanced approach that respects both confidentiality and the need for transparency.

Cost recovery

The DPO has the power to recover the cost of an investigation where the firm is found to have breached the Regulations. The aim of cost recovery is not to further punish firms but to ensure that the burden of investigation is borne by the responsible party and that firms are held sufficiently accountable for their actions. The recovery of costs will typically include expenses such as personnel hours, technical analysis, legal consultations, and administrative overhead. The DPO reserves the right to not seek the recovery of the cost of an investigation, but where cost recovery is sought, the DPO will be transparent about how the costs are calculated and provide the firm with an opportunity to review and respond to such a request before an order is issued. All monetary penalties will be payable for the benefit of the QFC Authority and not the DPO.

Effectiveness of regulatory action

The DPO provides quarterly reports to the QFC Authority Board Audit & Risk Committee, which encompass information regarding regulatory activities and formal enforcement actions. These reports may also cover specific concerns identified within individual firms or sectors where systemic issues relate to the protection of personal data have been identified and resolved.