Accountability Obligations under the GDPR

The GDPR expressly introduces a legal accountability obligation to European data protection law. While short in length and inconspicuous on a first reading, the new provisions are likely to have far-reaching consequences in practice.

1. Key Takeaways

(a) Codification of the accountability principle in the GDPR is in line with a **global trend** to make accountability a legal obligation.

(b) Under the **accountability principle as codified in the GDPR**, controllers will be required to implement appropriate technical and organisational measures to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR, and review and update those measures where necessary.

(c) **What measures will be appropriate in each case**, will depend on the nature, scope, context and purposes of the relevant processing as well as the risks for rights and freedoms of individuals.

(d) The GDPR text provides **very little guidance** as to what measures controllers will need to implement to discharge their accountability obligations. Further guidance in the form of codes of conduct, certification mechanisms and clarifications from the Art. 29 Working Party/ European Data Protection Board ("**EDPB**") can be expected.

(e) A **best-practice approach** for organisations to satisfy their accountability obligations would be to build and implement a structured privacy management program. But **less comprehensive approaches** may be appropriate as well, depending on the level of risk raised by the data processing.

2. Background

The notion of accountability is not new to privacy law and policy. It was formally introduced into data protection regulation in 1980 when it was explicitly included as a basic data protection principle in the OECD Guidelines. Since then, the accountability principle has been included in a variety of international data protection instruments as one of several core principles and is slowly (but surely) finding its way into national data protection laws.

While accountability used to be all about allocating responsibility for privacy compliance, it is now about requiring a proactive, systematic and ongoing approach to data protection and privacy compliance through the implementation of appropriate data protection measures - increasingly referred to as "privacy management programs". Various international data protection instruments are being revised to reflect that change.

3. Accountability under the GDPR

Article 24 of the GDPR codifies the accountability obligation. It requires controllers to:

- implement appropriate technical and organisational measures (including introducing data protection by design and by default principles where relevant) to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR; and

- review and update those measures where necessary through notably internal and external assessment such as privacy seals.

Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(a) What does this mean in practice?

Needless to say that this obligation is very vague and many controllers will rightfully wonder what measures they would be expected to implement. The GDPR itself provides very little guidance in this regard.

Article 24(2) provides that controllers should implement appropriate data protection policies where proportionate in relation to processing activities. Implementing those policies alone will certainly not achieve compliance with the accountability obligation. Rather, controllers will be required to implement a range of measures as needed to ensure compliance with all of their obligations under the GDPR. In addition, they must implement measures enabling them to objectively demonstrate such compliance. This requirement will need close consideration in practice. Controllers will need to thoroughly document their data protection efforts and, if requested, make such documentation available to authorities. Any data protection measures implemented will also need to be periodically reviewed and updated as appropriate.

Article 24(3), supplemented by Recital 77, provides that adherence to approved codes of conduct and certification mechanisms may help demonstrate compliance with the accountability obligation. Hence, controllers can expect codes of conducts and certification mechanisms to specify the measures required in order to comply with their accountability obligations.

Further guidance on the implementation of appropriate measures and the demonstration of compliance, including on how to identify, assess and mitigate risks associated with data processing, can also be expected from the EDPB.

(b) Accountability and the risk-based approach

The accountability provision is qualified by the so-called risk-based approach: what measures will be appropriate in each case, will depend on the nature, scope, context and purposes of the relevant processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals.

The more likely and severe the risks from the proposed processing, the more measures will be required to counteract those risks. According to Recital 75, processing which could lead to physical, material, or non-material damage would be particularly likely to constitute 'risky' processing requiring particular attention. Recital 75 further provides the following examples as potentially risky processing:

- processing that may give rise to discrimination, identity theft or fraud, financial loss, reputational damage, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;
- processing that might deprive data subjects of their rights and freedoms or prevent them from exercising control over their personal data;
- processing of sensitive personal data or data relating to criminal convictions or offences;

- processing for purposes of profiling;
- processing of personal data of vulnerable natural persons, in particular of children; and
- processing involving a large amount of personal data and affecting a large number of data subjects.

According to Recital 76, the risk must be assessed in an objective manner to determine whether there is a "risk" or a "high risk".

Further guidance on identifying and assessing risks of data processing and on identifying best-practice approaches to mitigate those risks will likely be provided by way of approved codes of conducts, approved certifications and guidelines issued by the Art. 29 Working Party/ EDPB.

Controllers undertaking the types of processing activities listed above or otherwise identified as 'risk' or 'high risk' would be prudent to carefully consider their obligations under the accountability provision.

4. Accountability and existing regulator guidance

Privacy regulators around the world are increasingly embracing the notion of accountability as a vehicle to drive privacy compliance within organisations (regardless of whether their laws currently codify the accountability principle). So far, the privacy regulators in Canada, Hong Kong, France, Australia and Colombia have issued "Accountability Guides" or "Privacy Governance Frameworks" intended to assist private sector (and in some instances, also public sector) organisations setting up appropriate processes and procedures to ensure privacy compliance.

Those documents have a lot in common and provide helpful (non-binding) guidance. The common thread in existing guidance is that organisations are expected to take a more proactive, systematic and comprehensive approach to privacy compliance. Some of the regulators go as far as to promote privacy management programs as the appropriate tool to ensure privacy compliance. To read more about the rise of the accountability principle and related regulator guidance, please refer to our "Accountability Series" on b:INFORM here.

5. Your Accountability Game Plan

Complying with the GDPR accountability provision is a complex task. The very basic Article 24 does not do justice to the overarching concept of accountability which essentially requires controllers to perform all of their data processing operations in compliance with the GDPR and to be able to objectively demonstrate such compliance.

(a) **A best-practice approach** for organisations would be to build and implement a comprehensive privacy management program. In a nutshell, this would include implementing:

- an internal governance structure which fosters a culture of privacy within the organisation from the top down;
- various adequate program controls to ensure compliance with the various GDPR requirements (such as personal data inventories/ records of processing activities, tailored privacy policies and notices, data breach handling procedures, security and retention policies, privacy enhancing measures by implementing data protection by design or by default when building new products or services, conducting data protection impact assessments when the processing is likely to result in a high risk, processes for selecting and managing data processors, etc.);

- processes to continuously monitor, assess and revise the effectiveness and appropriateness of the program controls.

(b) Those organisations wanting to start on a smaller scale (due to lack of resources or other reasons), would be well advised to take the following steps as a starting point:

- consider if they have the right level of expertise, training and a sufficiently senior individual accountable for data protection compliance within the organisation;
- put in place appropriate data protection policies addressing the key requirements under the GDPR;
- implement mechanisms such as spot checks or audits to monitor compliance with those data protection policies;
- devise processes for periodically reviewing and evaluating the effectiveness of data protection policies in place;
- document all of the above to be able to objectively demonstrate upon request their accountability in an organised and effective manner and in a way that is not disruptive to business operations; and
- follow any practical guidance from European authorities on the accountability requirements.

* * * * *

Please contact your usual Baker & McKenzie contact for a demo of our information governance tool iG360 designed to help in implementing a comprehensive privacy management program or for support in addressing your accountability obligations.