Securys

Privacy Operating Model

December 2022

Privacy made practical®

Contents

Introduction 3
Data Protection Officer 4
Privacy Office 4
Privacy Advantage 5

Introduction

One key challenge in establishing a properly functioning privacy programme is defining and instituting a privacy operating model which will support an organisation by

1. Identifying the functions required for effective privacy;
2. Determining how these functions will be resourced;
3. Selecting reporting lines and budget responsibilities for privacy functions;
4. Setting and monitoring appropriate key performance indicators; and
5. Integrating privacy into the wider governance and operations of the organisation.

Successful privacy programmes rest on three pillars: compliance, risk and competitive advantage. While differentiated, these pillars are of course also closely linked; it is important in designing a privacy operating model to avoid silos. Nonetheless, there are clear distinctions between the various components of a comprehensive privacy operating model. Most important of these is the separation of the advisory, audit and governance function of the data protection officer and the practical, supportive decision making functions of the privacy office.

This paper provides an overview of the Securys approach to meeting this challenge comprehensively. While organisations need a privacy function to comply with the law, embrace the ethical principles of data protection and fulfil the privacy rights of all, this paper sets out an enterprise approach which assumes a number of existing functions within the organisation. Successful privacy practice requires a degree of collaboration, co-operation and integration with these functions.

Securys recognises that not all enterprises are organised in the same way and so there may be some adaptation requited to fit different governance and operating structures. Privacy programmes cannot be launched and run independently of other functions and there are crucial co-operative and collaborative relationships to consider, in particular with the information technology, legal, risk and compliance departments, as well as the broader relationships with teams (including HR, communications and marketing) whose support is integral to the effective implementation of the operating model.

If you would like to discuss in more detail how the Securys model could be tailored to your organisation, contact us on privacy@securys.co.uk.

Data Protection Officer

The office of the data protection officer (DPO) drives privacy governance. This function is often described as "the embodiment of the regulator within the organisation" but can also be seen as the guardian and champion of the interests of the people whose data is being collected and managed by the organisation. The DPO is there to check that all processing of personal data within the organisation is not only compliant with relevant regulations but also properly serves the interests of the people to whom the information relates.

The DPO must be independent of decision making about processing; they provide advice and guidance – which the organisation is often legally required to heed – but do not approve processing or sign off on risk. By the same token they must be protected from sanction when questioning or challenging the organisation's processing of data. Most regulation requires that the DPO report directly to the most senior level of management; therefore to the CEO, Board or Chair. This reporting is intended to be both independent and constructively critical of operational privacy management and governance.

The DPO is also the interface between data subjects and the organisation; this is true both for external stakeholders – customers, suppliers, partners, shareholders and the wider public – and for employees and contractors. The independence of the DPO helps to guarantee those people access to the rights granted to them by legislation, which usually include information about processing, access to copies of data, correction of mistakes and erasure of unnecessary information, objection to processing and rights of appeal where decisions are made automatically.

Close collaboration between the DPO and the privacy office is needed to meet these obligations – it is the privacy office that prepares transparency notices, executes requests for data or the exercise of correction and erasure rights, and provides the interface with the business for objections and appeals. In this context the DPO acts to represent the individual and hold the organisation to account while the privacy office works for the organisation to meet its obligations.

Finally the DPO is the liaison with the regulator, acting to demonstrate compliance, to seek guidance and – in case of breach – to notify and inform.

Privacy Office

The privacy office is an operational risk and compliance function with a strong component of business support. Its role is to identify and document personal data processing across the organisation, assess operational and regulatory risk and recommend – and in some cases implement – appropriate risk treatments. This will include the preparation and maintenance of documentation required by regulation such as the record of processing activity, data protection impact assessments, legitimate interest assessments, transfer impact assessments, privacy notices and so forth. These documents also form part of the risk assessment process and feed into the wider organisational risk register.

The privacy office provides advice and guidance to the business on all aspects of privacy. It is responsible for preparing, maintaining and disseminating the organisation's privacy policies and procedures, which must be drafted with due attention to the advice and opinions of the DPO. Its advisory role also extends to reactive advice arising from questions from business units and functions, proactive advice resulting from investigation and assessment and the provision of procedural and policy training. Its active role includes the formulation and implementation of regular privacy training and awareness as well as the management of suspected personal data breaches and co-ordination with regulators.

Most regulation requires – and best practice always includes – the operation of privacy by design and default, i.e. the incorporation of data protection principles and practice into the fabric of all activities and projects which involve personal data from the outset. This requires the privacy office to be involved in all innovative and evolutionary change within the business whenever personal data are involved and should include formal processes for risk assessment and project decision making. The privacy office has a need

for technical resources – commonly referred to as privacy engineers – as well as privacy professionals with legal or risk management expertise.

Primarily a risk management and compliance function, the privacy office is best placed to report into the chief risk officer, where that role exists, and into the CEO or CFO if it does not. There is close co-operation between the privacy office, the legal department and the information security functions, but privacy should not report into either of these functions directly. Where privacy reports to legal there tends to be a disproportionate focus on regulatory paperwork and policy without sufficient pragmatic attention to operational risk and business need; by the same token, where it reports into IT the tendency across the whole organisation is to assume not only that privacy is an IT problem but also that it requires only IT solutions. Some organisations have effectively ended up with discrete privacy functions within both areas; as well as being inefficient this also leads to significant operational and compliance gaps.

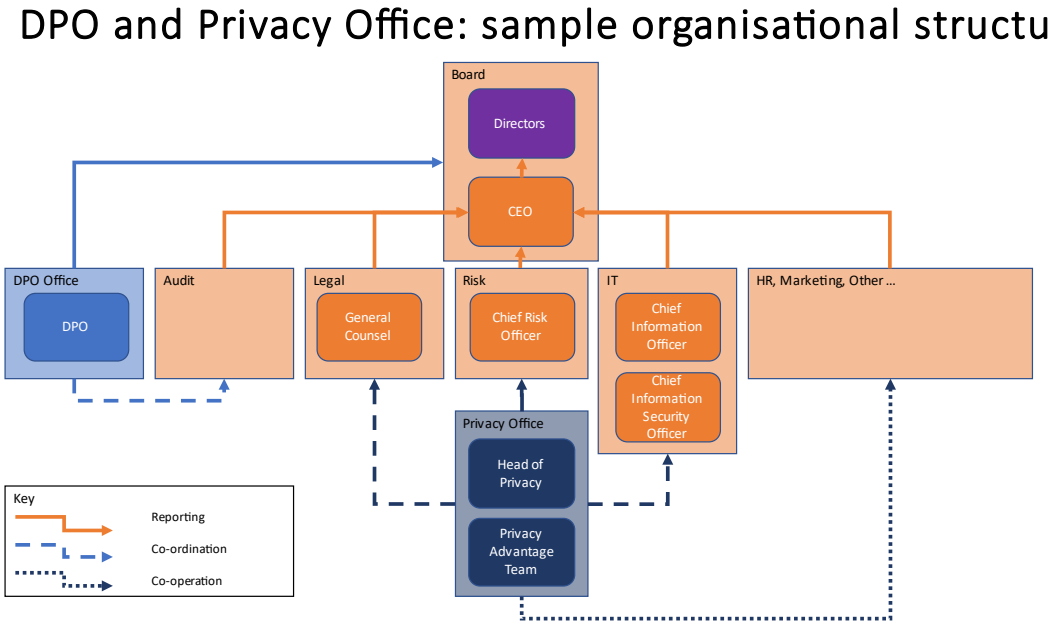
The privacy office is led by the Head of Privacy. This is an operational leadership role that requires both privacy and management skills as well as sufficient legal and technical knowledge to manage the interaction with the IT and legal functions. The Head of Privacy should be a peer of the CISO and a peer or near peer of the General Counsel.

Privacy Advantage

Organisations with significant consumer/customer bases or large workforces, especially in countries with strong employee privacy protections, can benefit from setting up a separate privacy advantage team as a sub-function of the privacy office. Working closely with marketing (for consumer customers) and/or HR (for employee recruitment and retention) this unit focuses externally and internally signalling the organisation's commitment to privacy – usually with some focus on outperforming competitors.

The signalling will be a mixture of conventional marketing and public relations, internal awareness training and work with product teams to improve the visibility of privacy to customers. This is commonly found in an e-commerce context, where the digital nature of the product, a large customer base and a high interaction rate allows different approaches to providing privacy information and enabling data subject agency to be tested. There is a feedback loop between the privacy advantage team and the privacy office itself, with joint work on transparency information and upwards flow of suggestions regarding privacy improvement from the advantage team into the privacy by design process.

Example of organisational infrastructure



Securys