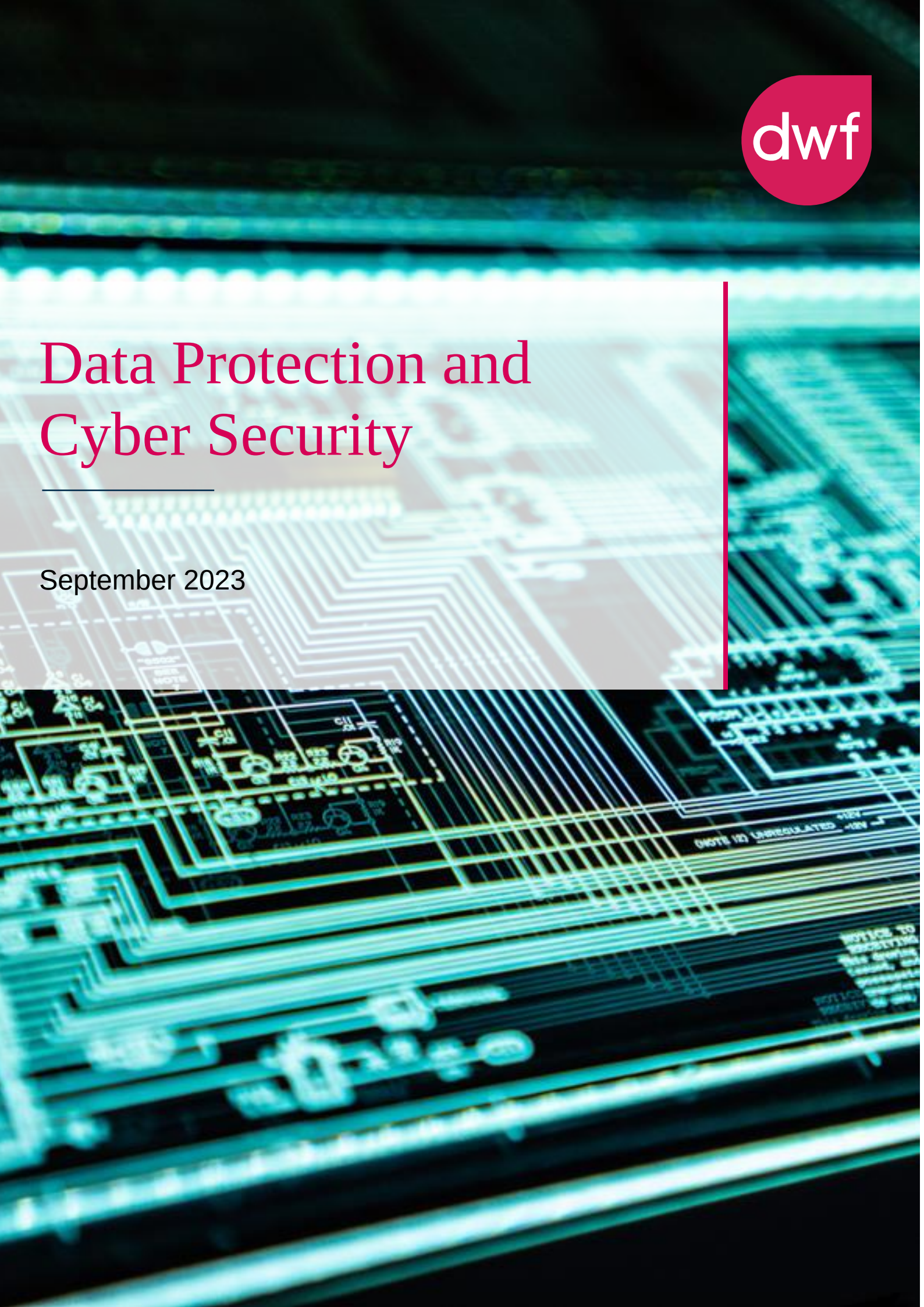


Data Protection and Cyber Security

September 2023

Contents


dwfgroup.com


DWF.Enquiries@dwf.law


linkedin.com/company/dwf


@DWF_Law

Data Protection and Cyber Security

DWF's legal and multi-disciplinary professional services business provides clients with global support on critical issues in Data Protection and Cyber Security. Our team includes legal advisors, management consultants, risk professionals, technologists and auditors who combine to provide truly holistic, end-to-end solutions.

Delivering meaningful, high-quality outcomes

With our dependency on technology and data, increasing volumes of regulation, raised awareness levels and the negative consequences of operational failure – Data Protection and Cyber Security resilience needs to be prioritised. It is crucial in order to withstand shocks and sustain our success. DWF are focused on helping clients to deliver meaningful, high-quality operational outcomes for Data Protection and Cyber Security, not 'ivory tower' legal advice or 'compliance for compliance sake'.

We do this by helping our clients to focus on the things that matter the most and assisting them with:

- Vision and strategy development for the handling, use and security of data and the digital environment, including the achievement of ethical outcomes and business purpose.
- Business transformation programmes that deliver Data Protection and Security by Design.
- Technology strategy, procurement and deployment including for new and advanced processing purposes such as profiling, biometrics, automated decision-taking and AI.
- Resilience, risk management and sustainable compliance to ensure the adoption of appropriate controls and accountability.
- Stakeholder relations including data subject rights requests, customer complaints handling and workforce training.
- Board and C-Suite engagement for corporate good governance, covering awareness raising through to support for effective executive decision making.
- Personal data and security breaches from the development of playbooks for incident response through to notifying breaches to affected people and the authorities.
- Crisis handling to make sure the right approach is undertaken in the most challenging situations, to mitigate loss and protect reputation.
- Regulatory investigations and enforcement actions including evidence preparation, advocacy and representation in court.
- Group litigation and class actions to resolve disputes and to defend against compensation.
- Due diligence to help maximise deal value in mergers, acquisitions, investments and corporate transactions.
- Horizon scanning and thought-leadership to help with issue spotting and to stay ahead of the curve.
- Tools and accelerators such as workflows, templates, PrivacyTech and SecurityTech solutions, to help operationalise outcomes and free-up management time.

What does a good approach to Data Protection and Cyber Security look like?

The right approach for gain and loss situations

Data Protection and Cyber Security issues arise in business in two broad situations: for gain, or for loss. In gain situations, organisations are seeking to drive benefits from the use of data and the digital environment; while in loss situations they are either prevented from using data and the digital environment, or their use is having negative effects, including through lack of resilience. The best approach to an issue can differ radically depending on whether it's a gain or a loss situation.

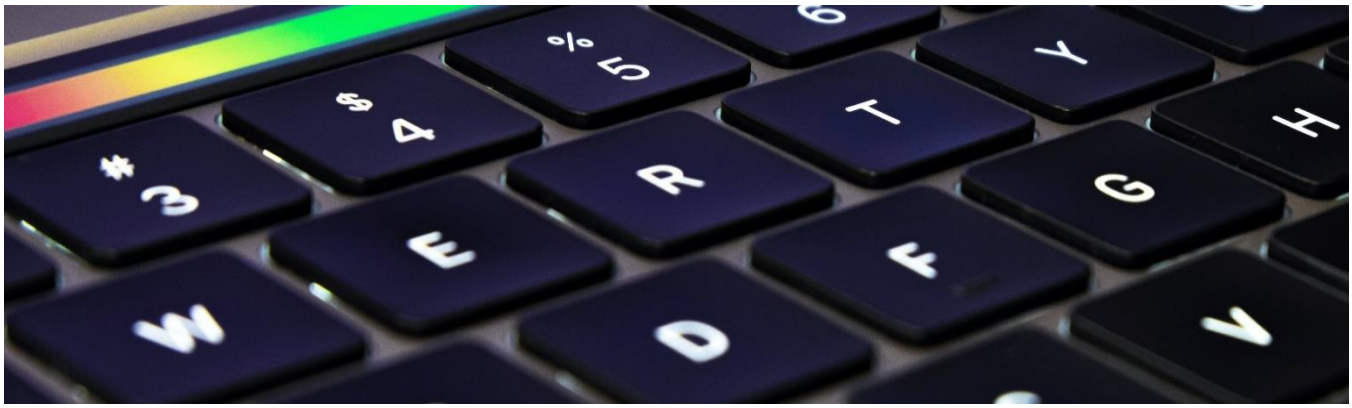
We always seek to understand the underlying context when designing and delivering our support to clients, to maximise the value and impact of what we do, and we believe in taking a balanced approach.

Our mindset is that data processing and technological developments have enriched the world in countless ways, serving humankind, freedoms, economic growth and prosperity. In gain situations we support our clients to achieve their business purposes and legitimate interests, helping them to innovate and grow – in balance with their obligations and mindful of the rights of others. In difficult situations, we bring a calm and ordered approach, helping to defuse and de-escalate problems and reduce loss, harm and damage. Our support extends to helping clients to better communicate their aims and objectives, including through constructive engagement and dialogue with regulators and special interest groups.

Understanding your Special Characteristics

No two organisations are the same. What makes them different are their Special Characteristics, which are their unique operating and environment features.

The Special Characteristics include the organisation's business sector; geographical location; legal and administrative structures; business operations, model and plan; culture and ethics; risk profile and appetite; prior legal and regulatory track record; and its resources. Achieving quality outcomes for Data Protection and Cyber Security, such as effective risk management, resilience and compliance, is always dependent upon understanding the impact of the Special Characteristics for data handling and the digital environment.



Achieving your goals on the things that matter the most

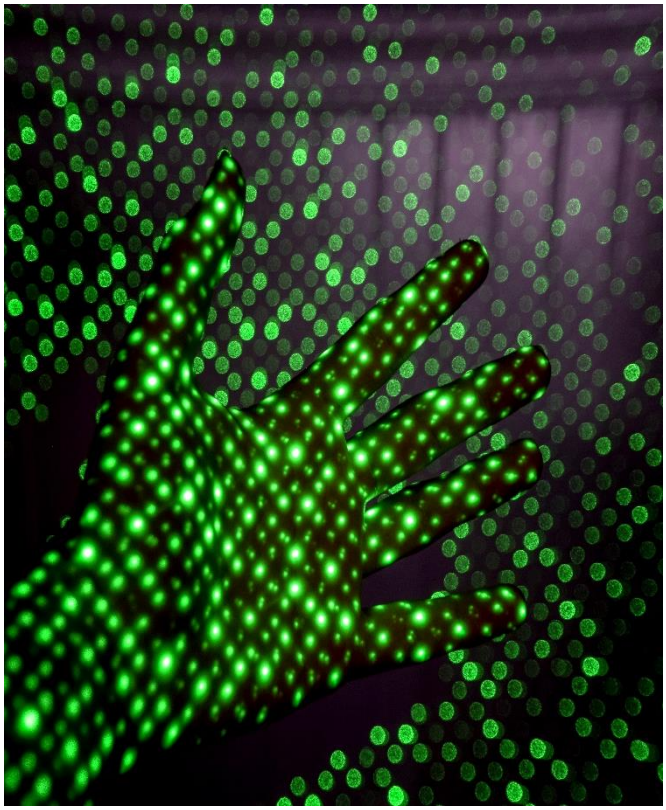
Although the law provides a baseline of outcomes that responsible organisations must achieve, their ambitions for data and the digital environment will extend much further than legal compliance. Delivering business purpose, achieving economic targets, acting ethically and maintaining the trust and confidence of stakeholders and investors are just as important in the setting of data and digital goals.

We always recommend taking a broad and holistic approach when determining goals and priorities, and we can help you through the process of identifying and refining them.

Being situationally aware

Organisations need to be situationally aware in order to be truly confident that major issues of concern are properly understood and addressed.

We track developments internationally, across industry sectors and in the legal system, and maintain engagement with the wider community of stakeholders who are invested in the achievement of good outcomes – such as privacy activists, worker representatives and consumer champions. We always feed-in these insights to our client engagements, providing benchmarks against which our clients can compare themselves and track their performance.



Addressing the technology and data layer

At the epicentre of the digital world and cyberspace are technology and data themselves. In order to deliver quality outcomes for Data Protection and Cyber Security, organisations must address the technology and data layers of their businesses and their supply chains. Governance models and paperwork by themselves are not enough.

Technical acuity and affinity are at the heart of everything we do. We have strong relationships with technology and data experts, including leaders in PrivacyTech, SecurityTech and AI, so that we can pinpoint the state of technological development to help guide clients on their tech and data strategies. Through our work, helping clients handle incidents and operational failures we have acquired deep understanding of the types of quality gaps in the tech and data layer that can cause serious business interruption, reputational damage and legal consequences.

Resilience and withstanding challenge and adverse scrutiny

The worlds of Data Protection and Cyber Security are ones where an organisation's position can be tested regularly by challenge and adverse scrutiny. These tests can occur on a planned or unplanned basis, for benign and malign reasons, through both internal and external channels. Benign, planned, internal testing can include the monitoring of controls by Internal Auditors and others performing risk management and due diligence functions. Malign and unplanned testing often arises from external forces, such as cyber criminals. Others operating along the spectrum of challenge and adverse scrutiny include disgruntled workers, whistleblowers, regulators, shareholder activists, upset customers, compensation claimants, the press and media.

We have broad understanding of the causes and dynamics of challenge and adverse scrutiny. We can help clients plan and prepare for testing situations and guide their responses in live situations, right through to representing their interests in the highest courts in the land.

Acting ethically and doing the right thing

The law tells organisations what they can do and what they cannot do, but it rarely answers the question 'what is the right thing to do?'

Many aspects of the use of new technologies and data processing techniques pose ethical dilemmas – with examples including profiling, tracking, automated decision-taking and data sale and monetisation. Our holistic approach to the issues supports the development of Data Ethics visions and strategies, and through processes of ethical stress testing and challenge an organisation can gain a better sense of confidence in its positions.

Our capabilities and services

Big litigation and dispute resolution

Data Protection and Cyber Security problems create fertile ground for large scale litigation and also low value, high volume individual claims. Our experience in these areas is unique. As successful defence solicitors on the first and largest Data Protection group litigation cases to hit the UK Courts, acting for Wm Morrison Supermarkets plc, and acting for British Airways plc, we can provide all clients with the confidence they need in 'class action' situations and for the handling of mass claims. Through all stages of the process, from initial 'pre-litigation' intimation of claims, all the way through to representation in the Supreme Court.

Our support includes:

- Litigation strategy, including the development of approaches to address the litigation style of the claimant firm.
- Identification of litigation funding options and mechanisms.
- Streamlining litigation, so that the most problematic challenges are handled efficiently and in a cost-conscious manner.
- Helping to manage publicity, alongside PR and communications teams.
- Providing assistance with and working alongside parallel criminal investigations.
- Providing assistance with regulatory issues that may arise, such as handling inquiries from the Information Commissioner's Office and sectoral regulators, including abroad.
- The management of employee and customer impacts.

Regulatory investigations and enforcement actions

The legal frameworks for Data Protection and Cyber Security are highly and actively regulated, not just by the authorities appointed under legislation, such as the GDPR and the Cyber Security Directive, but also by sector regulators, professional regulators and under Code of Conduct schemes.

We help our clients to navigate through all kinds of engagements with their regulators, and our track record includes advising on some of the leading enforcement cases for breaches of regulatory law.

Our support for clients includes:

- Making introductions into the regulatory system, through engagement with regulatory officers.
- Pre-clearance work, such as registrations, authorisations and approvals.
- Strategies for establishing and maintaining functions and offices that act as points of contact for the regulatory system, such as Data Protection Officers and EU Representatives.
- Assistance with the development of internal and cross-industry Codes of Conduct for compliance with regulatory requirements.
- Responses to regulatory and public consultations.
- Assistance with accountability obligations, including optimising the presentation of evidence.
- Advice and representation on all aspects of investigative processes and enforcement actions.

Incident response and data breaches

Every organisation is at risk from personal data and cyber security breaches. From large-scale cyberattacks to the loss of paper records – the range and scale of the threat to data security and business resilience is diverse. Our approach to incident response begins with prevention, through identifying and embedding appropriate controls that deliver operational resilience and demonstrate legal compliance. However, when incidents happen, we can support clients through all steps of the response and deal with all of the legal aftermath.

Our comprehensive, global breach management support includes:

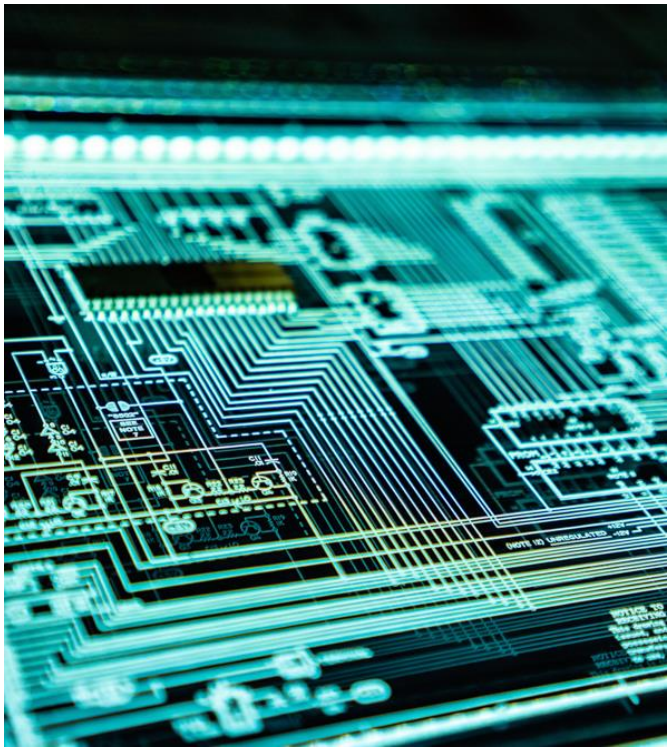
- Incident response readiness health checks and risk assessments.
- Scenario planning and threat simulation, including table top exercises and live testing of incident response processes.
- Optimisation of incident response plans, including the development of role-specific playbooks.
- First response services and tools, including 24/7 data breach hotlines and mobile phone notification apps, giving access to legal, media and forensic experts.
- Incident management support for containment, mitigation and recovery, including data recovery and evidence preservation, within a legally privileged environment.
- Breach notification support, including to people affected by an incident, regulators, law enforcement agencies, contracting partners, stock markets and insurance companies.
- Litigation support, ranging from injunctive relief, complex claims management and financial recovery, often provided against the background of regulatory investigations and parallel proceedings such as compensation claims.
- Insurance coverage advice in respect of standalone cyber policies and silent cyber risks coverage in traditional policies.

Business transformation and risk management

Our multi-disciplinary team have worked on some of the biggest Data Protection and Cyber Security transformation programmes and risk management projects in the market, including for GDPR compliance, to enable radical new business processes and to help remedy the worst cases of operational failure.

We provide clients with end-to-end, global support in these areas, including:

- The development of visions and strategies for transformation and risk management programmes, including for the use of novel technologies and in crisis situations.
- Maturity and current state assessments and diagnostics.
- Project planning, including governance and reporting structures; target operating models; roadmaps with milestones, deliverables and other KPIs; resource plans and budgets.
- Project management and programme assurance.
- The design of risk models and methodologies, and the performance of risk assessments.
- Controls design and implementation.
- Education, training and awareness.
- Monitoring and testing.
- Staff augmentation.
- Legal advice and opinions, including to identify legal requirements and to assess legal compliance levels.



Cyber Security strategy, operations and resilience

Cyber Security and operational resilience are conditions for success and safety in the digital world. The size of the benefits that organisations take from increased connectivity with staff, customers and supply chain partners through digital channels, is matched only by the size of the Cyber Security risks that they are exposed to in the ordinary course of business. These risks need to be understood and balanced in order to keep the organisation and its stakeholders safe from harm.

We help clients to understand and respond to cyber security risks in a manner proportionate to the unique circumstances of the organisation and the threats facing them. Our services include:

- Cyber Security vision and strategy development.
- Transformation support, including project management.
- Designing and embedding of standards, controls and risk management frameworks.
- Maturity and operational resilience assessments, including benchmarking.
- Threat and vulnerability assessments, including vendor risk management.
- Security awareness training and business culture change.

Sustainable compliance

Compliance is an ongoing requirement, not a moment in time activity, and organisations have to be able to prove that their compliance programmes are enduring. We help clients to sustain their compliance and demonstrate they are doing so, to the requisite level of proof. Our support includes:

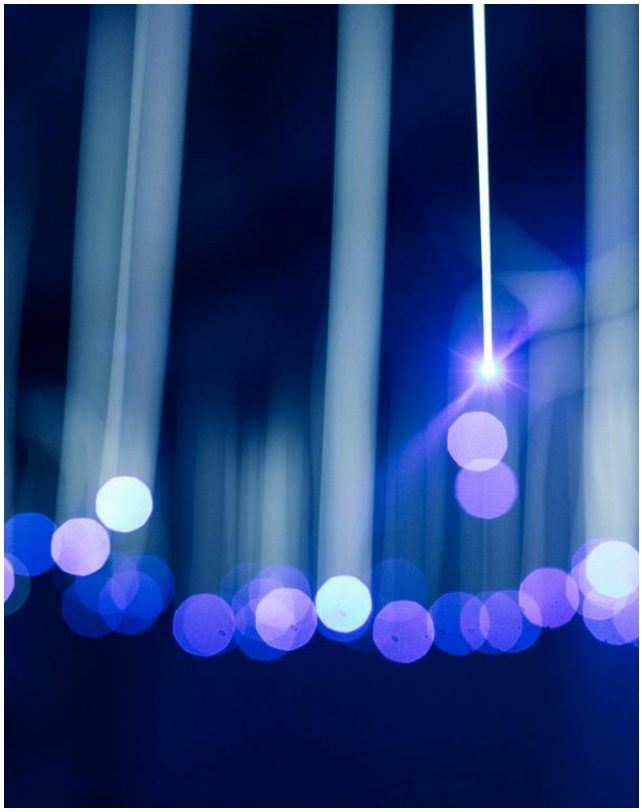
- Advice on legal and regulatory developments, trends and hot topics, to help keep clients' compliance activities focused, up to date and on track.
- Provision of compliance toolkits, including all of the artefacts that are needed for accountability purposes, such as Privacy and Security by Design frameworks; governance and operating models; risk assessment frameworks; policies, notices and contracts; controls libraries; playbooks; and workflows.
- Diagnostics for the assessment of operational, legal maturity and resilience levels and gap analysis.
- Training and awareness services, including e-learning platforms and online courses.
- Independent testing and monitoring of compliance levels, including audit and security penetration testing.
- PrivacyTech and SecurityTech strategy development, selection and deployment, to boost productivity and reduce legal risk.
- Staff augmentation, including the provision of Data Protection Officer and EU Representative services.
- Managed Services for compliance, helping clients to sustain their programmes on both an outsourced and co-sourced basis.

Rights handling

The scope and reach of the data subject rights have been significantly increased by the GDPR and other legislative developments, as has public awareness of the rights and how to use them. Organisations are experiencing increased volumes of rights requests and in some cases they are being used to support other complaints and legal action. We have extensive experience of dealing with the most complex rights requests, as external advisors on points of law and practice, through to the provision of end-to-end managed services.

Our support includes:

- Approach optimisation, to help clients to improve their processes and methodologies for the efficient and quick handling of rights requests – to minimise costs and disruption to their business, while maximising legal compliance levels.
- Toolkit development, including the provision of materials that can be incorporated into rights handling models, such as workflows; risk matrices; policies; guidance notes; template response letters; and other key correspondence.
- Staff augmentation, to provide you with surge capacity during busy times and crunch points.
- Managed Services, where we handle the rights request from receipt, through data collection, triaging and delivery of the required information, or from any stage in the process where you will benefit from outsourcing.
- PrivacyTech strategy and deployment, to help you to select the right technology partner for data search and retrieval, analytics, workflow management and process automation.



Data Protection Officer and Representative Services

Many organisations are required by law to appoint a Data Protection Officer (DPO) and others have elected to do so, while in some cases it is a legal requirement to appoint an EU Representative.

Our support includes:

- Target Operating Model design and advice, to ensure that DPOs and Representatives are properly resourced, skilled and tasked as well as situated in the best business location or function to ensure optimised service delivery and legal compliance.
- Outsourced services, where we can act as your DPO or your Representative, to be the impartial check on your organisation's compliance.
- Toolkit provision, so that the DPO and Representative have the right materials at hand to perform their roles.
- Staff augmentation to give your DPO and Representative additional capacity whenever needed.

Mergers and acquisitions, vendors and suppliers

Many organisations have acquired or inherited Data Protection and Cyber Security risks through their relationships with third parties, including through M&A activity and the building of their supply chains. Often the nature of third party risks are misunderstood, due to inadequate due diligence procedures, putting organisations at operational and legal risk.

Our approach to the assessment and management of third party risks helps clients to improve their operational resilience, and to maximise deal value in M&A and investment situations.

Our support includes:

- Advising acquiring organisations, venture capital firms, private equity firms and investors on the risk profiles of target organisations.
- The development and performance of fit-for-purpose due diligence frameworks for deal situations.
- The development of supplier and vendor risk management frameworks, including risk scoring, and entity segmentation and categorisation; step-by-step procedural requirements; contract formation and re-papering; and post-contractual due diligence.
- Operational testing of third party resilience, including penetration testing and auditing.
- Reputation and identity scoring and monitoring.
- Dark web monitoring.

New technologies and complex processing

Success in Data Protection and Cyber Security is contingent on understanding and mastering the issues that arise in the technology and data layers of the organisation, and through the use of complex data processing techniques.

Our support includes:

- Functionality analysis, to understand the operational and legal benefits and challenges that are involved in the use of use of new technologies and complex processing techniques, including the performance of risk assessments.
- Assistance with Privacy and Security by Design for new technologies and complex processing techniques, to maximise operational resilience and legal compliance, including the development of technology and data strategies and the creation of technology reference architectures.
- Advice on the state of the art, to help clients to make informed decisions on the deployment of new technologies and processing techniques.
- Product design and market making, to assist technology and data companies with the development of new products and services and roll out.

DWF is a leading global provider of integrated legal and business services.

Our Integrated Legal Management approach delivers greater efficiency, price certainty and transparency for our clients. All of this, without compromising on quality or service. We deliver integrated legal and business services on a global scale through our three offerings; Legal Services, Legal Operations and Business Services, across our eight key sectors. We seamlessly combine any number of our services to deliver bespoke solutions for our diverse clients.

dwfgroup.com