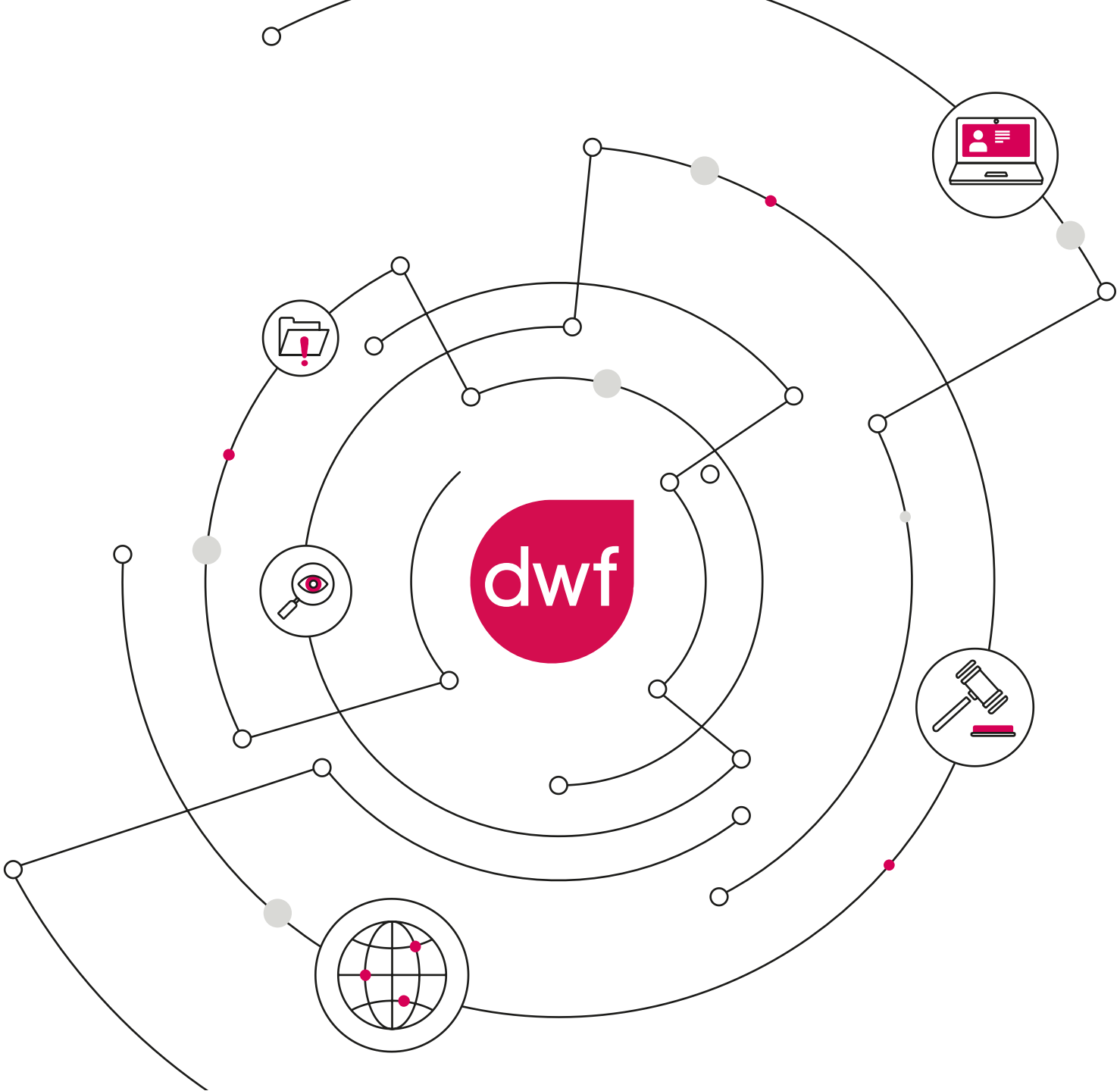
# Breach Counsel

## Cyber Security & Data Breach Services

End to end multi-disciplinary support for effective incident response and risk management

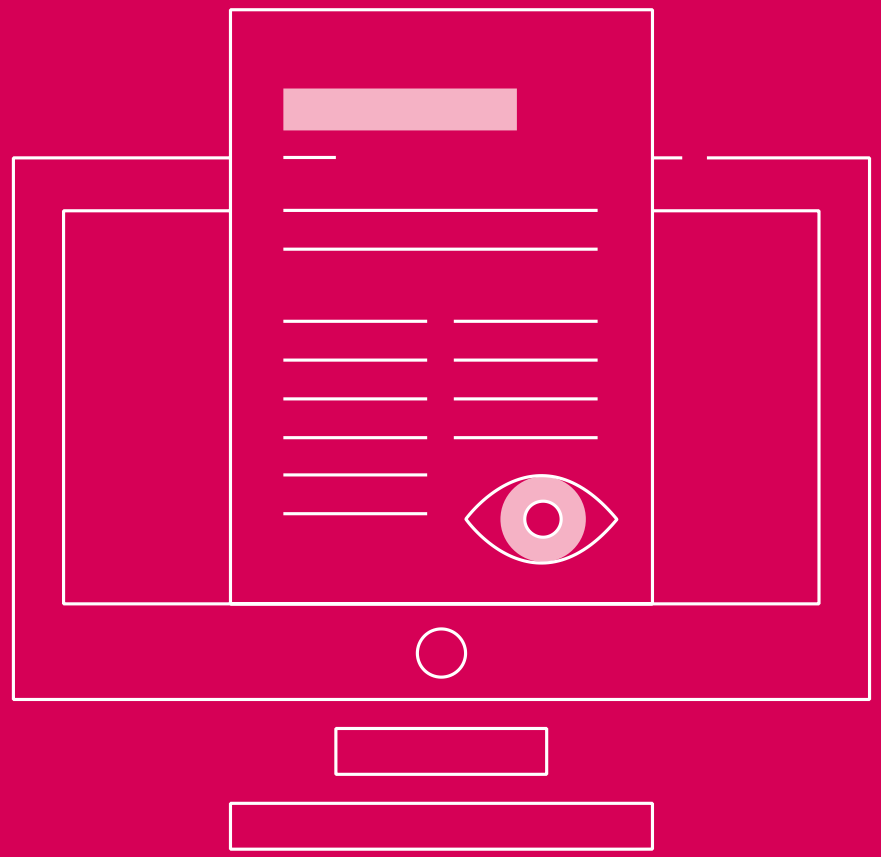
**dwfgroup.com**

GET IN TOUCH



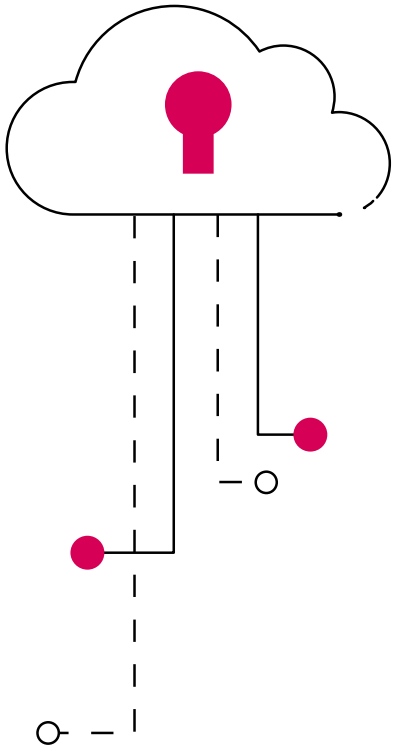
# Contents





For any breach counsel related queries relating please contact
**breach.counsel@dwf.law**

# What we are known for



## Crisis Management

Crisis management and incident response - Team members have a long, verifiable track record in providing professional services for incident response and crisis management after data and security breaches, as noted in the legal directories in previous years. Due to DWF's substantial insurance practice and our wider network of relationships with GCs, DPOs and CISOs, our caseload is substantial. Our Breach Counsel service, noted in the innovation section below, provides more details.

## Big Litigation

Our track record in very large scale litigation about data and security breaches is second to none, with credentials that include making new law in the Supreme Court. Our litigation practice continues to flourish. During 2021 we have defended many organisations from a wide variety of compensation claims for security breaches and data mishandling.

## Regulatory Litigation

Due to our crisis management and incident response work, we are advising clients on their regulatory reporting duties on almost a daily basis and the resulting investigations. Other areas of work in this area includes assisting clients in their response to regulatory investigations that result from Data Subject Access Requests and other rights requests; dealing with ICO audits; and dealing with the referral of DPIAs to the ICO, under GDPR Article 36. Related work includes advising and representing clients on FCA investigations and inquiries, which arise after personal data and cyber security breaches.

## Risk & Compliance

We support clients in the UK and abroad, across all sectors of the economy, with meeting the ongoing, daily challenges of data and security risk management and compliance. This includes embedding team members into client teams (e.g., as interim aDPOs); through to performing sentiment analysis on operational risks utilising our RAPID technology; end-to-end support on rights requests, including forensic data discovery and analysis utilising our DSAR Resolved service; and controls design and assurance. See the innovations section below for more information about RAPID and DSAR Resolved. During the reporting year, we did a lot of work on COVID-related matters (e.g., for NHS Digital and also supporting a leading retailer with the prioritisation of deliveries to people on the shield list); and international transfers (due to the landmark European court judgment in Schrems II). Our programmatic work has also shifted to providing consultancy support on CCPA compliance (US legislation).

# DWF enables effective incident response

## Rapid and robust response in highly stressful situations

Every organisation is at risk from cyber security and personal data breaches. From large scale cyber-attacks to the loss of paper records, the range and scale of the threat to data security and business resilience is vast. When a breach occurs, there is a need to respond rapidly and robustly, and ensure that legal and regulatory obligations are met.

We work with our clients to ensure that they respond appropriately to incidents and help achieve positive outcomes in relation to regulatory authorities, impacted individuals and other stakeholders.

Our Breach Counsel team has considerable experience in dealing with complex and challenging cyber security and personal data breach cases. Our support includes advising in relation to the recovery of business operations, undertaking investigations to determine root cause, and ensuring compliance with legal and regulatory obligations.

In addition to the above, our team is able to provide support post-incident, including advising organisations in relation to legal and regulatory strategy and large scale group litigation. We have a strong track record of representing clients in such circumstances, achieving the successful closure of regulatory investigations, and defending litigation.

## Key stages of incident response

- **First hour.** We will quickly assess the situation and provide initial advice and support.
- **First day.** We will help you develop your strategy for incident response, advising on "no regret" activities and instructing other experts on your behalf where they are needed to help with forensic containment, recovery and mitigation of the incident, and handling of PR and communications needs.
- **Within 72 hours.** We will advise you on your regulatory and other legal obligations, litigation risks and assist you in making any required notifications.
- **72+ hours.** We will provide necessary ongoing expert support in relation to your regulatory, technical, communications and legal needs.
- **Regulatory investigations.** We can represent you through all stages of a regulatory investigation including in relation to enforcement action.
- **Claims management.** Sometimes an incident will lead to subsequent litigation risks. We can provide advice and representation to you in relation to all aspects of litigation, including dealing with initial correspondence, DSARs, and any subsequent proceedings which are brought.
- **Post Incident Review.** We will advise you on how to improve your resilience and compliance to minimise further risks.

# Ranked as a leading data protection law firm by Legal 500 and Chambers and recognised for cyber security and data breach services:


"DWF is renowned for handling the contentious aspects of high-profile data breaches"

"DWF is sought out by clients from a range of sectors for advice concerning cybersecurity and data investigations"

# Why use DWF?

Our expert team has unrivalled expertise in handling cyber security and data breach incidents, having advised on some of the most complex and high profile incidents in recent times.

We understand the legal, regulatory security and threat landscape, allowing us to ensure that you respond rapidly and robustly when a data incident occurs.

We have established relationships with a large network of complimentary service providers across IT forensics and communications enabling us to provide seamless and joined up services.

We manage your incident response, utilising proven strategies and globally accepted standards supported by project managers and sector specific experts.

We track all steps taken by you in relation to the incident, in order to provide a complete account and assist with reporting and decision making.

We assist you with post-incident analysis and insights to help prevent reoccurrences and increase your resilience to incidents, thereby lowering your legal risk.

# Examples of recent cases

## Multi-disciplinary team

DWF's Breach Counsel team includes lawyers, cyber security professionals, management consultants and risk professionals. Our team has handled some of the largest and complex cyber security and data breach cases in the market and is recognised by the legal directories as a leading practice in this area.

01.

**Morrisons**

We successfully defended Morrisons in proceedings heard before the Supreme Court relating to a high profile data breach caused by a rogue insider.

02.

**British Airways**

We provided representation to BA in relation to large scale group litigation action brought following a data breach incident, and helped achieve effective outcomes for the organisation.

03.

**Food manufacturer**

We provided multi-disciplinary support in response to a ransomware attack by the Conti group, assisting the business to effectively recover from the incident and comply with its legal and regulatory obligations.

04.

**Global insurer**

We provided multi-disciplinary support in relation to a global data incident, ensuring a robust response to the incident and helping achieve the closure of regulatory proceedings across numerous jurisdictions.

# Methodology for success

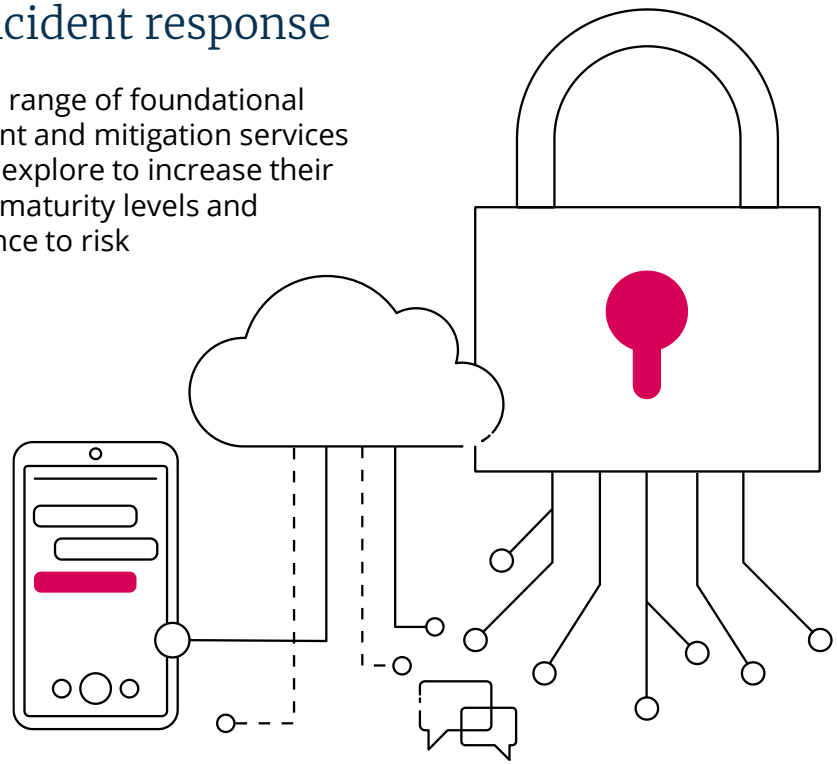
## Ransomware example

- **Understanding the attack**. Our immediate focus is understanding the nature and impacts of the attack, in order to ascertain how the incident occurred, the data affected and your legal, regulatory and commercial risks and obligations.
- **Understanding the threat actor**. We need to quickly understand the modus operandi of the attacker in order to provide advice on the appropriate strategy for engagement and insights on what can be achieved.
- **Secure recovery**. We will assist you in removing the attacker from your network and systems, thereby helping ensure that business continuity is achieved whilst preserving evidence, limiting impacts on affected data and preventing subsequent attacks.
- **Negotiating a ransom**. There are a number of reasons to engage with an attacker, for example in order to decrypt data, prevent data dumps, deter additional attacks and in some instances create tactical delay to secure systems. However, negotiations are sensitive and subjects to numerous risks. We can provide advice on how to engage appropriately with attackers whilst complying with relevant rules and restrictions.
- **Stakeholder management**. Ransomware attacks have far reaching regulatory, legal and commercial impacts and often become public knowledge. Good stakeholder management is essential in order to control the narrative and mitigate such risks. We can provide advice in relation to communications and project management services to cover all relevant workstreams and effectively control the incident.

# Cyber and data risk management

## Not just incident response

DWF provides a range of foundational risk management and mitigation services that clients can explore to increase their cyber and data maturity levels and improve resilience to risk



**DWF RAPID**. RAPID, which stands for Risk Assessments Powered by Insightful Data, is our cloud-based risk and resilience measurement tool, which provides immediate insights within seven key domains of cyber and data risk management. This is provided to clients free of charge.

**Playbooks**. Scenario-based playbooks can be prepared to further enhance the development of incident response strategy and the updating of the client's risk model. Playbooks can cover all types of cyber and data risks, to allocate and describe roles and responsibilities and expected behaviours; to plot core objectives of incident response against timelines; and to provide toolkits for management of all communications issues, e.g. template letters and web FAQs.

**Fire drills**. Aligned to key scenarios of risk, fire drills will put the organisation through its paces, in order to help assess and improve the client's readiness for handling of a real life incident. Options include role play and formal training.

**Third party services.** DWF have partnered with a range of third party service providers, to give clients a full service for cyber and data risk management. These include threat and vulnerability assessments, maturity assessments, penetration testing and audits. These services embrace all leading international controls frameworks, such as NIST and ISO.

**Tech and Data Leaders Forum**. This is our quarterly knowledge-sharing forum for clients, which takes place by webinar. Free to attend, the Forum provides cutting edge insights into the developments in the field of technology, data and cyber. The Forum is supported by a monthly updates newsletter.

**Helplines**. We can provide clients with free helplines, including on a 24/7 where specifically required. Helplines can be used for general, ad hoc queries, through to gaining support at the beginning of a real incident.

# Data management services

Our cyber security and data breach services are supported by leading data management and investigations software, tools and experts allowing for quicker and more effective services all in one place.

## Forensic Data Collection & Preservation

DWF have partnered with leading forensic collection specialists to preform forensic data collections both regionally and globally.

## Managed Review Services

An agile, scalable and multi-lingual managed review team with a variety of SMEs.

## Data Analysis

Our team of experts can solve complex data challenges when clients require objective analysis and reporting of structured data.

## Data Processing

Transforming forensically collected structured and unstructured data (emails, document, audio, chat messages etc.) into a format that can be analysed, reviewed and disclosed.

## Early Case Assessment (ECA)

Quickly establish the important facts early in a legal matter: key issues, key individuals, data 'richness' and the potential cost of review.

## Analytics, Review & DSAR Response

An experienced team of eDiscovery professionals with decades of combined experience. Access to industry-standard platforms with training provided.

# Specialist software

Technology and specialist tools are at the heart of the services we offer. DWF have selected, customised and created specialist tools which support our incident response, investigations and litigation support services, including but not limited to:

## Secure file hosting and collaboration

Collaborative working platform used for external file sharing, client portals and other solutions. In a data breach scenario you can use this platform to allow safe external file sharing and create a place to centrally manage the progress of the case.

## Contract reviews

AI Contract review software, which uses both AI and rules-based extraction to identify key information in contracts, including notification requirements, liability clauses and other relevant provisions thereby enabling you to quickly ascertain your contractual risks and requirements in a breach scenario.

## e-Discovery

Our document review platform provides powerful search, review and redaction capabilities accessible from your browser anywhere anytime and can be effectively used to review affected documents to analyse data.

# A global legal business

+30 global locations

+4,000 people

6 associations

### 3 offerings

Legal Services, Legal Operations and Business Services

### 8 sectors

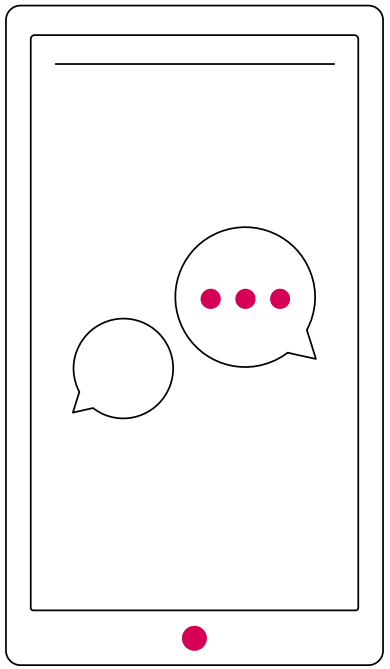
Built Environment, Consumer, Energy & Natural Resources, Financial Services, Government & Public Sector, Insurance, Technology, Media & Communications and Transport

### £380m revenue for FY23



Our locations Our associations

# Breach Counsel – Core Team



Stewart Room

Global DP&CS Leader

T +44 20 7645 4354
M +44 79 1914 4938
E Stewart.Room@dwf.law

Stefan Paciorek

Global DR Leader

T +44 20 7645 4148
M +44 75 2591 0538
E Stefan.Paciorek@dwf.law

James Drury-Smith

UK DP&CS Leader

T +44 20 7280 8821
M +44 79 1249 8512
E James.Drury-Smith@dwf.law

JP Buckley

Regional DP&CS Leader

T +44 16 1603 5039
M +44 75 1312 1776
E JP.Buckley@dwf.law

Ben Johnson

Partner

T +44 16 1537 1416
M +44 79 6855 9314
E Ben.Johnson@dwf.law

Euros Jones

Partner

T +44 20 7280 8928
M +44 78 7362 4305
E Euros.Jones@dwf.law

Tim Smith

Partner

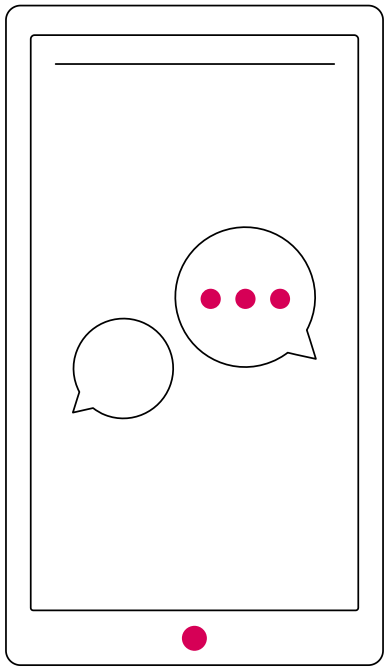
T +44 20 7645 4224
M +44 78 7280 5719
E Tim.Smith@dwf.law

Daniel Williams

Partner

T +44 16 1604 1681
M +44 77 4277 7400
E Daniel.Williams@dwf.law

# Breach Counsel – Core Team




[Jamie Taylor](#)

Senior Managing Director

T +44 16 1604 1606
M +44 77 1289 9712
E Jamie.Taylor@dwf.law



[Tughan Thuraisingam](#)

Director

T +44 20 7645 4224
M +44 75 2392 9354
E Tughan.Thuraisingam@dwf.law

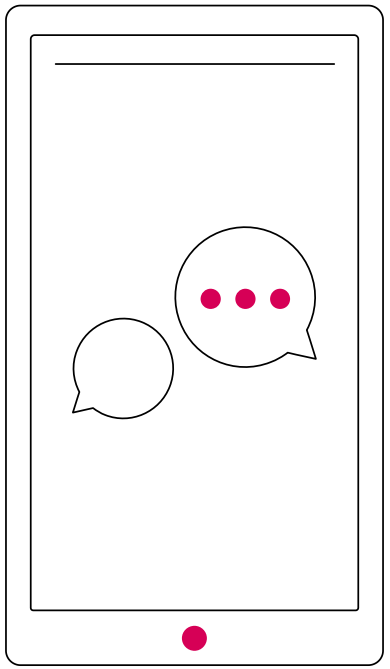


[Michelle Maher](#)

Senior Associate

T +44 16 1603 5112
M +44 75 4794 1330
E Michelle.Maher@dwf.law

# Breach Counsel – Core Team




Claudia Webb

Solicitor Apprentice

T +44 16 1838 0278

E Claudia.Webb@dwf.law



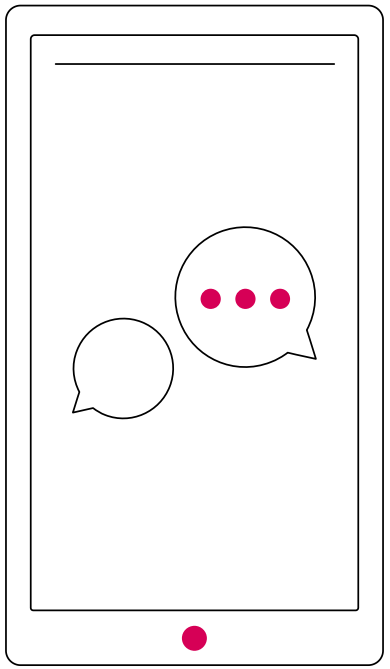
Sophie Broome

Solicitor Apprentice

T +44 16 1537 1488

E Sophie.Broome@dwf.law

# International contacts




Anne-Sylvie Vassenaix-Paxton

Partner (France)

T +331 4069 2651

M +33 6034 76561

E AS.Vassenaix-Paxton@dwf.law



Gerard Karp

Partner (Poland)

T +48 22 653 4200

M +48 502 184 707

E Gerard.Karp@dwf.law



Jörn Albrecht

Partner (Germany)

T +49 2112 1020 – 312

M +49 1511 5049 411

E Joern.Albrecht@dwf.law



Alejandro Griffiths

Partner (Spain)

T +34 9350 34868

M 606356118

E Alejandro.Griffiths@dwf.law



Francesco Falco

Partner (Italy)

T +39 0230 317999

M +39 0203 17984

E Francesco.Franco@dwf.law


## USA services

DWF have partnered with leading US law firms to provide first class cross-jurisdictional end to end services.

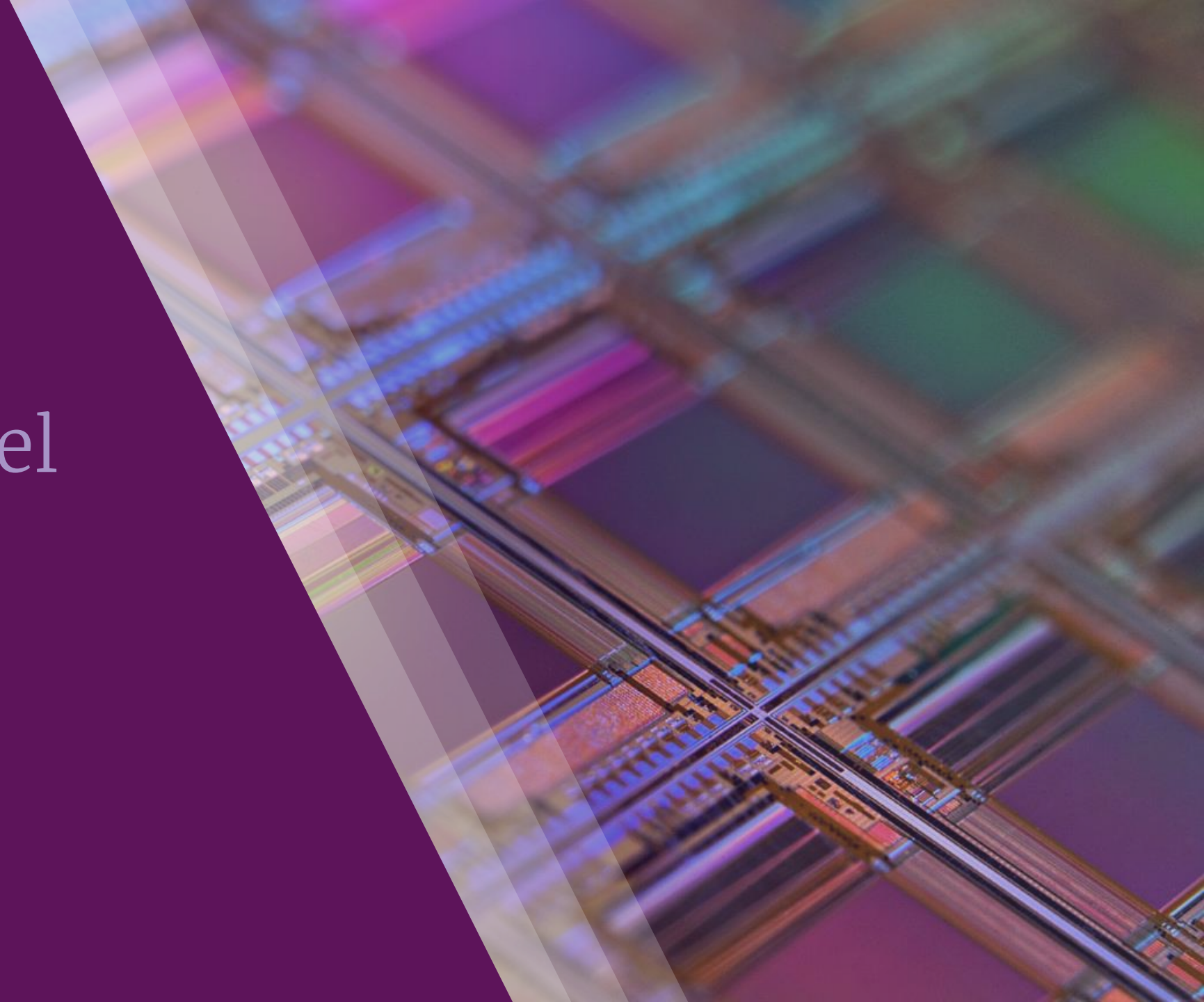
For breach counsel queries relating to Asia Pacific or rest of world please contact **breach.counsel@dwf.law**

For all other general queries please contact **DataProtection&CyberSecurityteam@dwf.law**

# Breach Counsel

**Annex 1 – Case Studies**

GET IN TOUCH



2022

## British Food Produce Brand

This client is a well-known British food produce brand who was subject to a major ransomware attack in early 2022. As a result of the incident, the client was unable to operate and/or manufacture goods, effectively halting their business. The client engaged DWF to provide both consultancy and legal services to respond to the incident and assist the client in becoming re-operational. DWF successfully assisted the client to re-commence its operations and manufacturing, whilst navigating its legal responsibilities, including duties to regulators and impacted individuals.

2021 – 22

## Food Packaging & Logistics Company

This client suffered a major ransomware incident in late 2021 which impacted all major systems and caused severe impact on operations. Following initial notifications of the incident the ICO opened an investigation into the matter. The client engaged DWF's breach counsel services to respond to the incident and engage with the ICO in response to their inquiries. Through submission of detailed information and written legal arguments on behalf of the client, DWF were able to successfully obtain a closure of the ICO investigation.

2021 – 22

## Global Telecommunications Company

DWF advised the client on two significant matters. The first involves a regulatory investigation following a suspected data breach by a third party processor involving the client's data. The second involves an enforcement action taken against the client by the UK Information Commissioner's Office (ICO) for alleged unlawful marketing practices. With respect to the second matter and as a result of the representations that DWF provided on behalf of the client, the ICO withdrew all of their allegations and did not proceed with taking formal enforcement action. The first matter is still ongoing.

2021 - 22

## Global insurance company: BEC

A global insurance company suffered an attempted £multi-million wire-fraud, facilitated through a Business Email Compromise attack, with an associated data extraction. We were instructed to advise on the strategy for incident response, including the performance of forensic investigations and the implementation of remedial actions. We engaged leading forensics experts on behalf of the client and provided recommendations to prevent recurrences. We prepared breach notifications for the UK and EU data protection regulators and for the UK financial services regulators, including industry bodies, and coordinated similar communications in the USA and Asia-Pac. Additionally, we performed an e-discovery review of the impacted data sets, against our methodology for understanding the risks to rights and freedoms to individuals within the meaning of the GDPR, and we have supervised a wider global e-discovery review for similar purposes in the other jurisdictions. Following our representations and legal arguments, all of the UK and EU regulators closed their investigations. We are currently engaged to oversee the development of a sophisticated communications strategy for the other jurisdictions, as well as coordinating the global legal strategy that builds upon the legal advice in those countries. The case is continuing.

2021

## Military components contractor: Ransomware attack

This contractor of very sensitive military components suffered a ransomware attack that resulted in the encryption of its systems. We were appointed to advise the client on the strategy for the response, including the engagement of ransom negotiators based in N.America; the performance of sanctions checks (including OFAC); the instruction of forensics experts; the restoration of systems from back-ups; the development of communications plans; and the reporting of the incident to the data protection regulator and impacted individuals. We project-managed the entire response and all of the professional services providers. Following engagement with the threat actor, clearance of sanctions checks, massive reduction of the ransom demanded, assurance being received about non-publication of data on the Dark Web and provision of proof of decryptors, the reduced ransom was paid and the client's systems were successfully restored. Following our representations and legal argument, the data protection regulator closed their case. The client received no adverse publicity.

2022

## Cloud Services Provider: Hafnium

We were instructed by a leading provider of Cloud applications with a global client base, whose MS Exchange environment, which was critical to their business, had been infiltrated by the Nation State-linked Hafnium group. We advised on incident response strategy including the instruction of forensic IT experts and the overall coordination of the compromise investigation. A malicious web shell was identified and removed and the attackers' attempts to communicate with the client's server were unsuccessful. As a result of decisive action, data exfiltration was prevented and the attacker was unable to gain persistence on the network. We provided strategic advice in relation to the hardening of the network environment to prevent recurrences. Following representations and legal argument to the UK and EU regulators their investigation into this cyber incident was closed.

2021

## US technology company: ‘risk to rights and freedoms calculator’

We advised a well-known US technology company on its legal obligations to notify and communicate a very large scale personal data breach under Articles 33 and 34 of the GDPR, which breach received international press attention. This engagement included providing a second opinion on the legal advice provided by other outside counsel and the development of a 'risk to rights and freedoms calculator', to help the client to assess the seriousness and impact of the breach on the individuals concerned.

2021

## Largest cyber breach settlement: British Airways

In 2021 we represented BA in the largest cyber breach settlement in the UK. We acted for BA in its defence and settlement of all civil claims arising from its high profile cyber-attack in September 2018, which affected 400,000+ customers. This was the first cyber breach group action under the GDPR.

2020

## Landmark success in first Supreme Court breach group action: Morrisons

In 2020 we successfully defended Morrisons supermarket in the Supreme Court in unique group litigation brought by 10,000 claimants, concerning the employer's liability for personal data breaches committed by a rogue employee. This was the first group litigation – and currently the only case - concerning personal data breaches to reach the Supreme Court. Our success in this matter has created new law and has significantly reduced the exposure of businesses to liability for security breaches caused by third parties.

2019

## Global entertainment company: Magecart threat vector

This client suffered a major ransomware incident in late 2021 which impacted all major systems and caused severe impact on operations. Following initial notifications of the incident the ICO opened an investigation into the matter. The client engaged DWF's breach counsel services to respond to the incident and engage with the ICO in response to their inquiries. Through submission of detailed information and written legal arguments on behalf of the client, DWF were able to successfully obtain a closure of the ICO investigation.

2019

## ICO investigations: Data broking

Whilst at their previous firm, Stewart Room, Mark Hendry and Simon Davis advised two leading companies in their responses to the Information Commissioner's investigation into the data broking industry, in their successful defences to enforcement action.

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.

We deliver integrated 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