WATERFORD TECHNOLOGIES

Expert Insight into your Data Management Journey, Challenges, Costs, and Solutions around eDiscovery, DSAR's & FOIA's

First-Hand advice from the experts.

Waterford Technologies and O'Leary Insurance with commentary from Matheson Legal

BRIAN O'MARA ACII

Account Executive,
O'Leary Insurances Ltd.

LAURA STOTESBURY

Head of Marketing,
Waterford Technologies

INTRODUCTION

The growing deluge of data in virtually all organisations makes it increasingly difficult to find and retrieve needed information in a timely and efficient way. Organisations that must find and produce data for legal or regulatory purposes, that must enable employees to find their own information in the course of doing their work, or that must reduce the amount of "live" storage to improve the efficiency of their systems and reduce risk, need a better way of addressing these problems.

The General Data Protection Regulation (GDPR) and the Data Subject Access Request (DSAR) have become synonymous with protecting the individuals' data privacy rights from misuse by businesses. However, there is no denying that responding to requests within the mandated 30 days is costing organisations a great deal of money and time.

In this article, Waterford Technologies in association with O'Leary Insurances highlight the issues in play and seeks commentary from leading Privacy Lawyer, Deirdre Crowley, Partner in the Innovation, Technology and Employment Groups in Matheson. We identify ways to simplify the data management journey, reduce risk, and reduce costs both human and financial. Throughout the article, we delve into the following topics.

- The legal cost of non-compliance with GDPR, The Freedom of Information Act (FOIA) and other privacy regulations?
- How email and file management providers can help mitigate risk and easily satisfy eDiscovery and Legal requests in a compliant and prompt manner.
- Non-Compliance During Covid- What are the costs?
- How insurance brokers can play a critical role in a business's planning and protection for GDPR and data breaches.

Since the implementation of GDPR in May 2018 Waterford Technologies has helped their clients with a steady stream of DSAR's but in the last few months, their clients are reporting a substantial increase in DSAR's, up 1300%. What this may be due to, whether it is individuals taking stock of what information is out there, an unanticipated consequence of the pandemic, (increase in redundancies, insurance claims, opportunistic), or something else: we can only speculate.

So, let us start at the beginning, what is involved in fulfilling a DSAR or FOIA request?

WHAT IS INVOLVED IN FULFILLING A REQUEST FOR DATA (GDPR OR FOIA)?

To fulfil the request a data protection officer or administrator must find every single piece of information about that person under the parameters specified in the request. It makes no difference if the information exists as structured or unstructured data. Manually searching for this information may mean logging onto various central systems and manually looking through email and file data, as well as having to ask employees if they have digital records of anything citing the requestor. That data then needs to be organised and redacted or shared as mandated, all of which takes tremendous time and effort.

Further, if anything is missed and the subject realises, they can complain. They can likewise complain if the tight calendar month deadline is missed without an extension agreement in place.

Deirdre Crowley of Matheson advises organisations "It's easy, but time consuming, to orgnaise a workable DSAR, FOI and privacy response plan. A robust and practice privacy compliance plan is worth it weight in gold when a contentious DSAR or data breach visits your door. Controllers' obligations to reply fully to DSARs is an inescapable part of irish data protection and GDPR compliance obligations. Failure to do so can result in protracted correspondence, significant management time loss, interractions with the DPC that may result in deeper dives into a contoller's privacy management generally with recommendations, compliance notices, fines, penalites and reputational damage to ensue. The cost of poor data compliance can result in a loss of confidence in a brand and significant financial cost in terms of downtime and legal costs. "

UNSTRUCTURED DATA AND GDPR

Unmanaged, unstructured data is a GDPR nightmare for DPO's. Why? simply because it is raw, unorganised data that cannot be stored in a predefined relational data structure. It is simply not easily organised or processed. The main culprits of unstructured data being email and file data such as pdf files and spreadsheets and other general office documents. Due to its unorganised nature and the fact that this data grows and grows in volume daily, it is a major challenge when it comes to companies and DPO's following GDPR requirements and fulfilling DSAR's.

Unstructured data accounts for approximately 80% of data. Imagine trying to filter through all that data to find all personally identifiable information (PII) of any EU citizens whether it be clients, partners, employees, ex-employees, or even suppliers. Not only do you need to find all PII's, then you will need to identify why it is stored, where it is stored, who has access to it, and with whom it has been shared. It is impossible to manage what you cannot see.

"When dealing with a DSAR, every piece of personal data on all company systems needs to be reviewed to understand what is in scope. WhatsApp groups, Microsoft Teams chats, business Skype and text messages may all be in scope. Where a document is identified as being within the scope of a DSAR, then it must be reviewed to consider whether third party data needs to be redacted. This is a time consuming, manual exercise, unless you have access to a digital services platform that can perform the searches for you. A large part of our work in assisting clients is working with our Digital Services Group in Matheson to search and redact many gigabites of data for the purposes of DSARs." Deirdre Crowley, Matheson

WHAT ARE THE TRUE COSTS OF HANDLING EDISCOVERY, FOIA, AND SUBJECT ACCESS REQUESTS?

The increased value of the data has meant that governments are establishing their own data protection laws such as GDPR, FOIA, CCPA & MiFID (The Markets in Financial Instruments Directive) which can come at a great cost for organisations if found to be in breach of these laws.

How much does a DSAR, eDiscovery, or FOIA investigation cost? That is a tricky question and the honest answer is, it depends. On a case by case basis, data subject access requests or eDiscovery costs can depend on multiple factors, including the size and type of data, the complexity of the review, and most importantly the type of data management solution employed. That is, whether companies review digital records manually, use a third party or utilise in house review.

Financial Cost

Some larger organisations can receive up to 500 DSAR's a month, there is an immense potential financial and human cost in having to respond to them.

Some of these costs are simply the personnel needed to complete requests. Other costs will come from having to seek legal help, with some businesses outsourcing more complex DSARs to legal firms. There could also be litigation costs and fines for non-compliance.

Claims and Hearings

Sometimes a DSAR or FOIA is just the prelude to a more complex or contentious matter. If the individual(s) in question want to take the matter further or are unhappy with the responses received, an organisation could incur costs related to court cases or dealing with regulators such as the Data Protection Commissioner, or their local equivalent. If the DSAR is related to a cybersecurity (incident such as a data breach), it is possible to insure against the cost via a Cyber Insurance policy.

HR Related Data Breaches

Deirdre Crowley of Matheson outlines what could potentially be on the horizon for Irish data controllers, "European organisations are experiencing a sharp increase in HR-related data breaches, not specifically related to DSAR'S but more because of poor HR security and compliance practices. The Irish Data Protection Commission is heavily involved in following these cases". A key take away Deirdre mentions is that:

> ***"data controllers should keep an eye on what the other European regulators are doing, as this is likely to be followed here. Breaches are happening that are attracting significant fines and those fines are around the improper processing of biometric data for time and attendance, for example, the improper holding of excessive personal data in respect to employees without carrying out the correct deletion practices and the implementation of improper retention periods."***

The legal costs of non-compliance with the GDPR can potentially be significant and we see the issue of HR related data breaches as a growth area now and into the short-term future.

Human Cost

Alongside the raw financial costs, there is also the human cost to consider. Preparing for DSAR requests will be a collective effort among data privacy officers, information technology teams, and business leaders. To make decisions companies must understand their data, be able to log requests, collect and review the information before they can securely deliver it to the requestor on time and with ?.

On average they might have to deal with some 50 emails per DSAR all with varying types of attachments and all needing redaction of PII concerning other parties. And then there is always the worry that something has been overlooked.

Costs of Non-Compliance during Covid

Non-Compliance with GDPR during Covid prove costly. Organisations are processing a high volume of special category health data that normally they would not be processing at all. Because this special category data is so sensitive it could attract higher fines and penalties which is a cause for concern. If you are an organisation which processes more personal data than what is needed on a return to work form, such as health data, you need to proceed with caution.

Deirdre Crowley of Matheson notes that "We do expect to see investigations into the proper handling of health data in the workplace because of Covid." Deirdre advises that specific compliance procedures should be put in place to deal with this unusual data processing activity. Such measures include a specific COVID privacy policy and if necessary, Deirdre recommends that the employer conducts what is called a Data Protection Impact Assessment to risk access the need to process such sensitive data to provide a safe place at work.

DSAR AND FOIA HANDLING – TOP TIPS

DEFINE ROLES & RESPONSIBILITY

make sure everyone in the organisation knows how to play their part in the DSAR process

VALIDATE EXISTING PERSONAL DATA HELD

For organisations with substantial amounts of data in their possession, this is best undertaken using electronic search technology.

ESTABLISH POLICIES & PROCEDURES

review and revise existing policies and procedures to set up an efficient process for handling DSAR and FOIA requests which include the search element.

TRAIN STAFF

Staff need to be able to identify potential DSAR's and understand what their role & obligations are with regards to the response.

MINIMISE PERSONAL DATA

securely erase personal information that is no longer needed, in line with the organisation's data retention policy.

CONSIDER EFFICIENCY MEASURES TO IMPROVE DSAR RESPONSES

organisations may want to explore the assistive technologies to improve their GDPR & DSAR preparedness.

UNDERSTAND YOUR DATA

what personal data is held and processed for the organisation's data subjects

CONSIDER CYBER INSURANCE

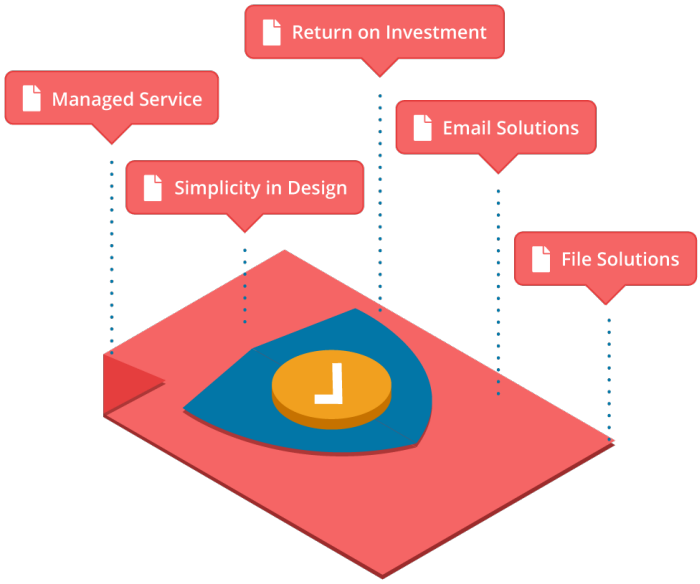
a good policy will cover costs related to DSARs if linked to a cybersecurity incident such as a data breach.

HOW TO DEFENSIBLY DISPOSE OF EMAIL AND FILE DATA?

"An essential element of good information governance is being able to dispose of information that is no longer needed and doing so in a way that can be defended to regulators and the courts. Defensibly deleting information reduces corporate risk and lowers storage management costs."

- Osterman Research 2020

Deirdre Crowley of Matheson advises that "the only way to defensibly dispose of email and file information is to fully anonymise and encrypt the information, such that any third party that tries to access the data cannot identify any data subject from it. If information is anonymous it falls outside the scope of GDPR."



HOW LONG ARE COMPANIES ALLOWED TO KEEP EMAIL AND FILE DATA?

The question that is on everyone's mind is how long they can keep their email and file data. There are different retention periods depending on the data that you process, statutory periods such as annual leave records or break records- you simply refer to the relevant statutory period. If there is no statutory period then you simply ask yourself if there is an exception arising in the data protection act that allows you to retain the data. For example, if there is potential litigation attached to the data you can retain that data for the purposes of getting legal advice, longer than the standard statutory period but it very much depends on what is contained in the email or the file data. There is no one size fits all answer for data retention, it is very much dependent on what data is in scope.

Deirdre Crowley of Matheson advises that your privacy statement is very important. "Your privacy statement states the type of personal data that you process and the length of time that you retain that data. A privacy statement is a legal obligation. Under article 13 of the GDPR". Implementing a data protection policy is not required by law but Deirdre states that it should be implemented as best practice outlining an organisations retention schedule, saying what can be kept and what can be deleted.

HOW ARCHIVING CAN HELP

For many, the sheer complexity of requests, combined with a lack of adequate systems in place, necessitates an extension to the deadline, which equates to a corresponding increase in resources. To help reduce the number of resources spent on DSARs and ensuring GDPR compliance organisations need to set up mechanisms that enable them to quickly and accurately find all the data concerning any individual wherever it is held.

According to a recent survey by Osterman Research (sponsored by Waterford Technologies) - "Archiving business records is the first step in enabling a proper defence during regulatory audits, legal actions, and in other situations in which older content must be retained."

Email archiving software can simplify how an organisation can access and act on personal data that exists in their email.

Here is how

DATA ANALYSIS

An archiving solution will help an organisation find its data, the good, the bad and the ugly! Locate it and understand it; where it is, how long it has been there and what is in it. Archiving software makes unstructured data searchable.

DATA POLICIES

Setting up retention, deletion, and compliance policies in an organisations email archive can ensure compliance is kept and continuous monitoring in the archive can ensure policies are working well and tested.

MAKING DATA DECISIONS

It is not enough to just have policies in place, organisations must be able to reduce, delete, and redact personal data. Email archiving can facilitate the deletion of redundant cold, obsolete data that is clogging up your server and the archiving of data that is not used but needs to be kept under retention policies

DATA ACTION PLAN

Archiving can enable an organisation to store personal data in a compliant manner. As outlined by GDPR, considerations need to be able to implement retention controls and policies which can be individualised by department or branch. Through data, analysis organisations can report on how long they are keeping personal data.

HOW CAN CYBER LIABILITY INSURANCE ASSIST WITH GDPR?

In every crisis, there is an opportunity. Unfortunately, the mass migration towards working-from-home during 2020 has created a significant opportunity for Cyber Criminals. According to Interpol, "with organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption".

Where previously an employee could ask a colleague if a particular email attachment or link "looked right," now they have to pick up the phone and explain it to the same colleague. That alone could persuade an employee that opening the attachment is a risk worth taking. Criminals are banking on employees being more lax at home when it comes to following well-established internal processes.

Brian O'Mara of O'Leary Insurances cautions that it would be naive to presume that a 'traditional' insurance programme will protect a company against GDPR-related incidents. Insurers do not want to cover what they are not charging a premium for. Any 'grey' areas where their wordings were not clear are being eradicated as insurers update their policy wordings – many now insert clauses removing all doubt that there is no 'Cyber' cover under other policies.

Cyber Insurance is the name given to the all-encompassing product that protects companies from the likes of data breaches, system interruption from ransomware and even cybercrime losses. The name is somewhat misleading given many such policies will cover accidental data breaches or loss of data in hard copy format - they don't just respond to a hack of your IT system.

O'Mara commented that most Cyber Insurance wordings will include language noting cover for GDPR fines, but only as long as they are legally insurable. The last few words are key here; such fines are likely to be punitive in nature and as such, it may not be legal for insurers to pay out - similar to how it is not possible to insure against a speeding ticket. He advises that there will need to be case precedent in each country in the EU to obtain clarity on this point, however, for now, it is best for companies to presume there is no cover for GDPR fines.

However, here in Ireland there have been very few GDPR fines to date. Instead, clients of O'Leary Insurances have been incurring other costs related to data breaches, which can be covered by a comprehensive Cyber Insurance policy. For example:

- IT experts looking to identify the source of the breach, as well as restoring systems
- Crisis experts co-ordinating notification to regulators such as the Data Protection Commissioner and to those individuals affected by the breach (this cost alone can be significant)
- Setting up a call centre to handle queries related to the breach
- Identity theft or credit monitoring costs e.g. if sensitive data has been released
- Defence costs and claims relating to the breach, as well as cost of attending regulatory hearings if necessary
- Public relations/crisis handling costs if the matter is going to result in negative publicity
- Lost income to your business while handling the fallout
- Some policies even cover a review of your systems post-breach to prevent re-occurrence

A GDPR fine is not guaranteed after an incident. However, some or all of the above costs will be incurred. O'Mara gave the example of a client who used a third party to run competitions for their customers. That third party was hacked and lost customer data – mainly names and email addresses. Also, the ability to call on experts to help handle the breach should reduce the likelihood of being fined or taken to court. The breach had to be dealt with by the client as Data Controller, and it cost insurers almost €40,000. This included call centre costs and an expert co-ordinating the correspondences with the DPC and those affected customers, and it was resolved to everyone's satisfaction. That was money well spent as far as both insurers and the client were concerned, given one of the client's main competitors was featured in national newspapers as they too were affected by this breach.

THE IMPACT OF THE PANDEMIC - WHAT ARE THE LONG-TERM EFFECTS?

Data protection law has not changed because of COVID-19. Organisations still have the same legal duties to comply with the GDPR, FOIA and other Data Protection Acts.

The pandemic has forced tens of millions of information workers to work from home, a situation that has caught many off guard. This change of work environment has meant that many IT and information governance teams are no longer archiving their data properly. The reduced ability to archive business records during the pandemic is playing a significant role in the reduced ability to meeting compliance obligations

Not archiving all necessary business records during the period of the COVID-19 crisis is going to have long-term ramifications for businesses that fail to retain and protect their business records properly.

SUMMARY

It is clear from the expert opinion noted in this article that the data privacy and cyber threat landscape is rapidly changing. The loss or disclosure of personal or sensitive data is still a primary concern for organisations. However now more than ever businesses are increasingly facing threats to their ability to conduct normal operations.

Data controllers are being hit from every angle; increase in DSAR's, FOIA's and malicious threats like ransomware are on the rise and businesses cannot ignore the unintended disclosure and human error risks. Business must protect themselves on all fronts. A combination of Electronic Archiving equipped with WORM (Write Once Read Many) Technology and Cyber Insurance can offer an extra line of defence.

Unlike backup and legacy worm archives, Waterford Technologies offers an affordable archiving solution that includes WORM technology at no added cost as well as built-in content indexing and discovery search for DSAR and FOIA requests.

Any prudent company should strongly consider purchasing Cyber Insurance to cover gaps in their insurance programme. It is the safety net if all internal processes fail i.e. human error. Taking out a comprehensive policy removes much of this risk from the company balance sheet.

COMPANY PROFILES

O'Leary Insurance

Insurance Brokers & Consultants, Est. 1961

O'Leary Insurances have aligned with premier insurers to provide cyber products which go above and beyond to provide cover solutions to all businesses presented with modern-day cyber threats. There is a wide disparity between policy wordings, you very much get what you pay for. They have designated Cyber experts in each office that would be happy to help discuss how Cyber insurance can protect your business.
O'Leary Insurance Group will consider all cyber risks from across a wide range of industries and their insurance partners boast a broad appetite and flexible approach to cyber underwriting.

If you would like a quote or more information on these covers or other relevant business insurance packages please contact one of their experienced insurance brokers at cyber@oli.ie.

Matheson

The law firm of choice for internationally focused companies and financial institutions in and from Ireland.
Established in 1825 in Dublin, Ireland and with offices in Cork, London, New York, Palo Alto and San Francisco, more than 740 people work across Matheson's six offices, including 96 partners and tax principals and over 515 legal, tax and digital services professionals. Matheson services the legal needs of internationally focused companies and financial institutions doing business in and from Ireland. Our clients include over half of the world's 50 largest banks, 7 of the world's 10 largest asset managers, 7 of the top 10 global technology brands and we have advised the majority of the Fortune 100 companies.

For more information contact- cork@matheson.com

Waterford Technologies

Waterford Technologies is a global provider of automated email and file management and eDiscovery focused solutions. They endeavour to help clients meet their email and file - archiving and compliance requirements to reduce risk and to address eDiscovery requests easily, quickly, and successfully.

Founded in 2000, their simple vision started with the idea that there is valuable business information stored in a company's email system, not just in the email content, but in context of the ways email moves through a company.

Waterford Technologies has built its reputation on our ability to deliver, scale and be flexible. They bring all of these characteristics to bear when delivering solutions to customers both in pre & post-sales.

Waterford Technologies provides their customers with robust and scalable data management solutions to meet their requirements for eDiscovery, active monitoring, control, visibility, storage growth management and retention policies across their largest sources of unstructured data.

Contact info@waterfordtechnologies.com for more information.