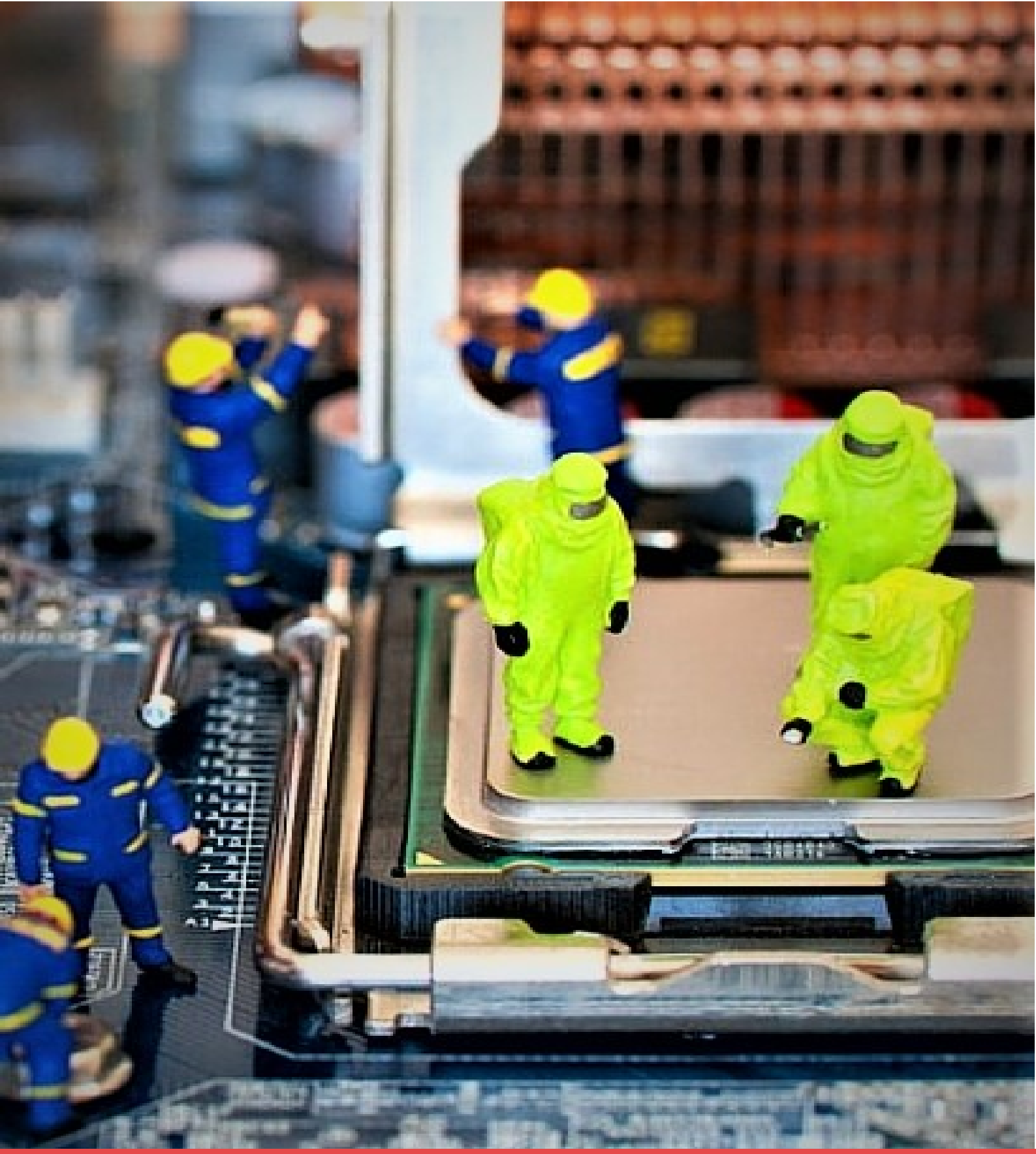

GDPR: The Health & Safety of Personal Data

IMPACT PRIVACY

Bringing privacy to life

Foreword

If European lawmakers were out to set records, the General Data Protection Regulation (GDPR) possibly stands out as being the most widely discussed and analysed single piece of legislation ever introduced. Ironically, social media has hugely facilitated this discussion, particularly twitter (#GDPR) and Linked-In, where countless commentators continue to contribute to an on-line discussion that dissects and analyses each of the GDPR's 173 recitals and 99 Articles.

The volume of noise about the GDPR reflects not only the breadth and depth of its application, but also the global impact it is having, on digital commerce specifically. However, this belies the fact that the data protection revolution started more than two decades ago, with the European Union's 1995 Data Protection Directive, which sought to ensure data protection became a core regulatory obligation affecting all business across the entire European Union.

However, the revolution had a false start. A failure of the lawmakers to ensure data protection principles were uniformly enforced across Europe, adapted to keep pace with rapid technological change, and given extra-territorial reach to reflect the global free-flow of data, amongst many other things, meant data protection was not taken as seriously as was intended.

The GDPR is the evolutionary change which, whilst firmly rooted in the original directive, is ensuring data protection becomes the compliance priority it was always meant to be and creates a formidable framework for the protection of individuals with regard to the processing of their personal data in the digital age.

The story is familiar, and in this short paper a correlation is drawn between the development of law and practice in health & safety, and the similar (but quicker) trajectory in privacy law - a correlation I have been making for some time. Importantly, it allows four key predictions to be made about what GDPR will mean for business in the years to come, so allowing the insightful to plan, prepare and stay ahead of the rapidly developing digital curve.

Léon Atkins
Dublin, September 2018

(This whitepaper was first published in January 2018 and has been re-published)

Industrial revolution to digital revolution

The industrial revolution brought unprecedented change to the way in which people worked and contributed to the growth of national economies. In the space of just 150 years, starting with the invention of the Newcomen's first productive steam engine, progressive industrial development shifted not just the UK economy, but that of other nations, away from small-scale and artisan production to massive scale, centralised, and factory-based output.

In doing so, huge and unretractable changes to the social, economic, physical and spiritual landscape were made, laying the foundations for the modern society we live in today.

Some two hundred years later, the digital revolution is similarly making a transformational impact on our everyday lives. Except this time, the pace of change is swift – very swift. It has been less than seventy years since the first commercially available computer, the Ferranti Mark 1[1], was released. Twenty years' later, Intel released the world's first microprocessor[2], and as little as twenty years ago, the dominant digital corporations, like Facebook, Google and Amazon, either didn't exist or were in their infancy.

Yet, just like the industrial revolution, its digital successor promises to make the same huge changes to our society, whether it is how we communicate, how we relate to one another, how problems are solved, or how services are provided. And as we enter the next stage of the digital revolution, with the likes of blockchain (distributed ledger technology), cryptocurrency and IoT (the Internet of Things), how we transact with each other, at every level, will soon be unrecognisable from even the turn of the century.

Controlling evolutionary side-effects

Many may reflect on the industrial revolution as having been inevitable, promising, and overwhelmingly beneficial. Whilst this might be the subject of many conflicting points of view, it is not controversial to acknowledge it also heralded industrial servitude, accidents and disease.

These side effects led forward-thinking constituents and activists to overcome the huge power wielded by the emerging industrial elite and persuade lawmakers that industrial conditions needed changing for the overall good of society and the protection of human rights and values. In the UK, the birthplace of the industrial revolution, this was first manifested in the Factory Act 1802[3], which sought to protect pauper apprentice children from unduly harsh working and living conditions. What then followed were successive reforms which brought about greater controls over the workplace environment, with the primary aim of protecting workers and the public from dangerous working and other practices. This lead was soon followed by other nations, such as the US where unions pressed for federal safety regulation, which started with the introduction of workers' compensation laws throughout the US in the early 1900's[4].

In both the UK and the US, a seminal moment arrived in the 1970's, with the introduction of OSHA in the US and, in the UK, the Health & Safety at Work etc., Act 1974 (the "1974 Act"). These laws, and others like them, transformed the approach to safety. Indeed, the UK's 1974 act was described as a "bold and far-reaching piece of legislation"[5] by the first Director General of the new Health & Safety Executive. Moving away from prescribed and detailed regulations, the 1974 Act introduced a system based on goals and principles, supported by guidance and codes of practice. By doing so, it shifted responsibility for defining and responding to industrial risk from the legislators to business itself, whilst at the same time creating legal expectations on which the

[1] https://en.wikipedia.org/wiki/Ferranti_Mark_1
[2] https://www.intel.com/content/www/us/en/history/historic-timeline.html
[3] See the "History of the HSE": www.hse.gov.uk/aboutus/timeline/index.htm and "History of Occupational Safety and Health" http://www.historyofosh.org.uk/timeline.html
[4] In 1911, the State of Wisconsin was the first to adopt a workmen's compensation act. Under workers compensation laws a worker need not prove negligence on the part of the employer, and the employer's three common law defences are eliminated, but the quid pro quo is that the workers compensation is limited.
[5] "Thirty years on and looking forward" – The Health & Safety Executive

public at large could rely for pursuing liability, and the state could rely for prosecution. Today, laws like this throughout the world provide a framework that seeks to provide protection to peoples' safety, provide access to compensation for harm they suffer, and prosecute individuals and businesses causing that harm.

Now the side effects of the digital age are starting to become apparent, as well as examined and imagined for the future, and by far the biggest side effect comes from how our personal data is harvested and used by those to whom we give it – wittingly or unwittingly. Fortunately, this was identified early and so, since 1970, when in Germany the first ever data protection law was implemented, there has been a growing and generally accepted response to the need to protect our fourth dimension: the information that is personal to us.

Most recently it has been the European Union that has led law-making in this area, and the EU's General Data Protection Regulation (GDPR), which comes into effect on 25 May 2018, represents a significant evolution in privacy law, just as OSHA and the UK's 1974 Act impacted workplace safety practices.

In much the same way as safety law recognises the need to protect our physical and mental welfare, the EU, through the GDPR and its predecessors, recognises the need to protect natural persons:[6]

"*The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the "Charter") and Article 16(1) of the Treaty on the Functioning of the European Union provide that everyone has the right to the protection of personal data concerning him or her.*"

With this statement, the GDPR goes on to make it clear in its subsequent recitals that a strong and coherent framework for data protection is required, backed by strong enforcement, and that people should have control of their own personal data. There must be a balance between allowing the digital revolution to flourish and the rights and freedoms of the personal data on which it is grounded. You can almost hear the social movement of the industrial revolution uttering similar words.

Orientation versus direction

So, whilst the background to the GDPR sets the scene for the thesis that it could be regarded as the health & safety of personal data, the substance of the GDPR and its likely impact on how personal data is managed ensures the thesis is demonstrated.

Firstly, there is relatively little granular prescription in what a processor of personal data must, and must not, do. It is much more of a framework of privacy governance and control (as the recitals to the GDPR themselves acknowledge), underpinned by six guiding principles[7] - that personal data must be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Building on these six principles, the GDPR provides 99 Articles of regulation text setting out the detailed expectations that must be met. At first you might be forgiven for believing this will provide all the detail needed, but more informed reading will tell you this is absolutely not the case. Recital 77 of the GDPR (amongst others) underscores this:

[6] GDPR Recital 1

[7] GDPR Article 5 – Principles relating to the processing of personal data

"Guidance on the implementation of appropriate measures and on the demonstration of compliance…especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood or severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer."

Just as with the UK's 1974 Act, the GDPR is not intended to be the answer, but instead the compass – you are either heading the right way, or you are not. This allows the principles of the GDPR to be promoted in a way that can be fluid, dynamic and efficient, responding rapidly to a fast-paced environment of change, particularly in the digital arena, whilst ensuring the general direction of travel remains the same. Safety law has been able to respond to a rapidly changing industrial environment in much the same way by reason of its flexibility - and the fact the 1974 Act is still in force today is a testament to its success in this respect.

A risky business

As any safety practitioner will attest, the fundamental principle of safety management is firstly to dispense with the risk (don't do it at all, or do it differently) and only if this is not feasible, should measures then be taken to reduce the risk of the operation.

It should be no surprise that the GDPR also focusses on risk (in fact the word "risk" appears more than 70 times in the text of the Regulation) – in particular, the risks presented to the rights and freedoms of natural persons in the processing of personal data which could lead to physical, material or non-material damage. These risks may include (extensively, but not exhaustively):

"discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects."[8]

So, in essence, where the risks to our rights and freedoms outweigh the benefits of the data processing activity, then the processing activity must stop or be changed. This is a principle firmly embedded in the concept of the Article 35 data protection impact assessment, which requires:

"*an assessment of the necessity and proportionality of the processing operations in relation to the purposes*".

This is further reinforced by the need for a data processor to consult with its supervisory authority if the processing activity represents a high risk – anticipating the possibility that the supervisory authority may deny the processing operation if the risks have not been adequately mitigated.

Characteristically, the GDPR does not indicate how risk should be measured, but in keeping with the spirit of the framework that has been adopted, each supervisory authority is required to publish a list of processing operations that require an assessment, allowing an ongoing evolution of the risk-based approach that keeps pace with technological development.
Against this background, it is not surprising that the risk element of the GDPR has given rise to its call for "data minimisation" as part of principles relating to the processing of personal data[9]. If you aren't processing the data, then it doesn't present a risk. The less data you are processing (or the less processing you do), the less risk there is. So, in future data privacy professionals must consistently challenge the need to process

[8] The GDPR – Recital 75

[9] The GDPR – Article 5, paragraph 1(c)

personal data at all, and if so, why and for what benefit.

All this means the response to the GDPR should not be to achieve compliance. Instead it should be about managing risk. Organisations will have to understand the risks processing personal data brings, obtain assurance about the systems in place to manage the risk, and make decisions about how risk gaps will be addressed. Claiming "compliance" with the GDPR will demonstrate a fundamental lack of understanding of what it is trying to achieve, just like trying to achieve compliance in safety is rather missing the point:

"*While the rapidly changing economic and political environment has thrown up new challenges in the form of new responsibilities and new demands, the central task remains to minimise the risk of harm and create a society where risk is properly appreciated, understood and managed."*[10]

Cost of failure

There seems little doubt that the GDPR will give rise to a significant increase in the risk of both prosecution and legal claims arising from the processing of personal data, and this is a path well-trodden by the impact of safety legislation.

For instance, in the UK the 1974 Act has arguably become a framework for the prosecution of safety offences, rather than simply a means for facilitating the management of safety by exhaustively defining the specific requirements for safety assurance. The very fact an individual has suffered an injury in the workplace is usually a demonstration that the required safety standards have not been met, putting employers very much on the defensive.

Whilst in a small minority of jurisdictions the local enactment of the 1996 Data Protection Directive has in some ways ensured that prosecution for privacy breaches has evolved to operate in a similar way to prosecution for safety breaches, the introduction of the GDPR will likely ensure the continuance of that trend, with greater consistency across all of the jurisdictions to which it applies, and most likely more prosecutions. In this context, the six principles embodied by the GDPR have to be seen as clear outcome-based measures – the KPIs of successful management of personal data processing risk. So, regardless of the systems adopted and the investment made in them, if the outcome does not meet expectations, then defending a failure will be very hard indeed.

And failure will be costly. The potential cost impact to an organisation of getting it wrong still dominates the GDPR headlines, with fines moving to maximum levels of between two and four percent of global turnover (or €10million to €20million if greater). This is where there is definitive divergence between the GDPR and safety laws, because the potential GDPR fines are far greater than those for safety breaches[11].

If that wasn't enough, in addition to the potential for prosecution by supervisory authorities, under the GDPR natural persons will be able to directly pursue personal claims for breaches. Such claims will be capable of being made in respect of non-material damage, meaning it might validly be predicted that the significant cost of prosecution will be far outstripped by the cost of private claims, fuelled by the development of claims farming and a much greater understanding by data subjects of their rights and remedies.

This prediction can be substantiated by evidence of what has happened in the context of personal injury claims arising from workplace accidents. Not only has a huge legal industry developed from the prosecution of such claims, but the value of these claims has dwarfed the value of criminal prosecutions for safety breaches. Bearing this out, in 2014 the UK's Health & Safety Executive reported that the total value of fines collected from business in respect of safety breaches in the 2014/15 year was less than £20m[12]. However, the value of employer's liability claims paid in 2014 far exceeded that figure at £839m[13]. Even with higher maximum fines, introduced in 2016, the total value of fines collected in 2016/17 barely reached £70m.

[10] "Thirty years on and looking forward" - The Health & Safety Executive

[11] Sentencing Council "Health and Safety Offences, Corporate Manslaughter and Food Safety and Hygiene Offences Definitive Guideline" – 1 February 2016. For organisations, up to £10m fine for health and safety breaches; corporate manslaughter, up to £20m. In the United States, OSHA Penalties are far less significant, with the current maximum penalty being limited to US$129,336 per violation (see www.osha.gov/penalties).

[12] http://www.hse.gov.uk/statistics/enforcement.htm

[13] Association of British Insurers – UK Insurance Key Facts 2014. In the US, in 2007, workers' compensation insurance cost $85bn [*Workers' Compensation Benefits, Coverage and Costs* – National Academy of Social Insurance]

Of course, claims for workplace injury are covered in many jurisdictions by compulsory insurance, the premiums for which are an accepted variable overhead for the insured business. It is still a cost, and the insurance market penalises employers who do not manage the underlying risk properly by raising the cost of individual premiums.

However, regardless of cost, this net of insurance for data protection risks is still immature, notwithstanding the GDPR and other rigorous national laws[14]. Cyber-policies, whilst now commonplace, are not data liability led and are relatively untested when it comes to coverage. This is equally true when it comes to Directors & Officers' Liability insurance. So, for the time being, the expectation must be that such claims will, by and large, be met directly by businesses without the buffer of insurance.

The issue of indirect costs should not be ignored in this discussion, and in the context of safety management, the recognition and measurement of the impact of workplace injuries have for a very long time been a significant driver for investment in safety practices. The understanding and influence of the indirect cost impact of data breaches will similarly continue to develop over time, but it is difficult to see how the GDPR will do anything other than serve to accelerate this, with the indirect benefit of fuelling investment in effective data and privacy management.

So, making the case for effective management of personal data processing risk will be far easier than it was in the past, and the cost implications of GDPR failures might give some clue as to how organisations may choose to prioritise their management of such risks.

Value of success

It's widely recognised, and understood, that good health & safety practices bring very positive outcomes to a business, and society as a whole[15]. In the business context, as well as lowering costs, it is credited for increasing productivity and quality, as well as reducing absenteeism and employee turnover. This of course lowers costs for business and improves efficiency, bringing a compelling business case to investing in, and properly managing, safety programmes.

So, there should be little doubt that good corporate privacy programmes will also bring benefits, the most obvious being the ability to demonstrate to stakeholders (customers, shareholders, funders, regulators, and employees), that personal data and privacy is both taken seriously and managed well in the organisation, making the business a more attractive proposition generally. Within this stakeholder group, it's arguable the most tangible benefits will be driven by customers. The level of awareness they have of their privacy rights is likely to increase, especially if a breach of those rights might give rise to compensation; this will be accompanied by a corresponding raising of expectations in respect of the levels of fairness and transparency adopted by business in the collection and use of personal data. All other things being equal, businesses that are the most fair and transparent should have an advantage over their competitors.

A benefit that perhaps hasn't been so widely associated with an effective response to the GDPR will arise from the implementation of the strong data governance principles which, ultimately, the GDPR absolutely requires be adopted[16]. Unsurprisingly, the universal data governance principles are entirely consistent with the personal data processing principles of the GDPR, as they call for:

- integrity
- transparency
- auditability
- accountability
- stewardship
- checks-and-balances
- standardisation
- adoption of change management practices[17]

By adopting these principles, an organisation moves toward ensuring its overall data supply chain can be better trusted and relied upon. Not least, this is because its provenance is tracked and traced, its quality is measured, it is more efficiently delivered, and is subject to less uncontrolled

[14] For example, the California Consumer Privacy Act, and Canada's PIPEDA
[15] See the British Safety Council's literature review: the business and benefits of health and safety – May 2014
[16] See, for example, Articles 24 and 25 – technical and organisational measures
[17] The Data Governance Institute

intervention. This matters since all decision making by an organisation is based on data inputs, the quality or accuracy of which directly impacts the decision they are supporting. So, in much the same way as good safety practices improve productivity performance and quality, good data practices should ensure higher quality data and thus better decision making, improved operations, and effective standardised and transparent processes.

Responding to the GDPR will require an organisation to review its data management practices. In doing so, it should take the time to identify opportunities for improving the data supply chain, not only to ensure the expectations of the GDPR are met, but also to realise the inherent value in more accurate, and so more meaningful, data.

A model for GDPR management

Making a comparison between health & safety on the one hand, and the data protection principles embodied in the GDPR on the other, may seem a challenging concept. Yet, it is a plausible comparison and, by doing so, we have seen it is possible to understand the likely evolving impact of the GDPR, and so develop planned and effective responses.

If this is the case, then it should be possible to look to safety management practices and adapt the framework within which they operate for the purposes of delivering the expectations of the GDPR.

For example, one accepted, as well as tried and tested, model for fundamental safety management is known as "Plan, Do, Act, Check", an approach designed to help deliver effective safety arrangements. This approach is highly relevant to developing a response to the GDPR and can be easily adapted for the delivery of a well-managed and successful GDPR programme, as briefly illustrated below:

"PLAN"
As a first step the business must define its policy in respect of personal data processing. What position will it take generally, what key standards will it adopt and what are the expectations of those subject to the policy. This must then be followed by the development of a plan for the implementation of the policy.

Both the policy and the plan must be effectively communicated and adequately resourced and have, as part of its objectives, the securing of commitment throughout the organisation to the key aims of its policy in respect of personal data processing. This will be critical for building and sustaining a positive culture in respect of personal data processing in the organisation, without which the GDPR programme may ultimately fail to deliver its objectives.

"DO"
As already identified in this paper, risk is a central theme within the GDPR, which calls for a risk-based approach to be adopted when designing a GDPR programme. This means identifying and understanding the personal data risks existing in the organisation's business processes, before then assessing them and building effective controls, in line with the expectations of the GDPR. These responses then need to be documented, implemented, and then managed.

They will further need to include discrete processes and procedures that support the overarching policy of the organisation, and which have been developed in response to the specific risks presented. These in turn need to be adopted, and the personnel who are expected to deliver them, adequately resourced and trained.

"CHECK"
Measuring performance is critical to ensuring that issues are capable of being identified before they arise and cause problems, so a system of performance measurement will be fundamental to a successful GDPR programme and helps underpin assurance.

This means systematically monitoring business processes, as well as periodically reviewing them for effectiveness. Audits will also need to be conducted to provide assurance that the relevant policy, processes, and procedures are being adhered to.

As part of the "checking" process, systems must be adopted that allow issues to be freely raised internally within the organisation but outside of the formal monitoring and audit process, to ensure risks are continually identified and addressed.

"ACT"
It is not enough to just measure performance; it needs to be reviewed and, when things go wrong, lessons learnt and acted upon.

As with health & safety, if things go wrong once, it must be treated. This means ensuring issues or incidents are thoroughly reviewed and analysed, and adequate treatments designed and implemented - if something has gone wrong once, it cannot go wrong again.

An important analogy

So why does this matter? It matters because the application of the analogy helps predict key developments for the management of data privacy (whether because of the GDPR or otherwise), which in turn can help organisations understand how best to prepare. This gives rise to four clear predictions:

Respect privacy, or pay…
The expectations of the public, customers, consumers, and employees, in respect of the protection of their privacy, will continue to grow. The unfair and opaque processing of personal data will be tolerated less, and, most critically, their knowledge of their rights, and remedies, will become more universal. Today, people readily identify safety risks and won't tolerate them. Tomorrow, the same will be able to be said of privacy, and laws coming after the GDPR, like California's Consumer Privacy Act will underpin personal data rights.

Stakeholder expectations will grow…
Consequently, privacy issues will quickly become a standing board-room agenda item. Failure to properly respond will represent an ever-significant risk to the operations and success of an organisation, and the stakeholders (including regulators) will expect that every board owns the risk and ensures there is an adequate response. How the risk is being managed will need to be communicated to the stakeholders, and over time the expectations of the stakeholders in respect of both the maturity of management, its success and how it is reported, will increase significantly. So, expect more substantive and detailed public commentary coming from boardrooms in respect of privacy systems, initiatives and performance.

Systematic management of the risk…
The need for assurance at board level will drive the adoption by organisations of strong privacy management frameworks, like the one illustrated earlier in this paper, which systematically provide assurance that throughout the business privacy risk is being properly managed. These systems will have organisation-wide impact and comprise key elements that:

- **establish** privacy policy
- **identify** privacy obligations and risks
- **develop** plans to address the risks and achieve privacy policy objectives
- **implement** operational plans and controls
- **evaluate** performance and reporting
- **manage** non-compliance and improvements

In turn, they will be built around organisational leadership, commitment, and strong privacy culture.

The rise of the privacy professional…
Finally, the management of these privacy issues within an organisation will very quickly need to evolve from being a legal compliance issue or an IT issue, to an operational data management issue, supported by privacy professionals who manage a privacy compliance framework that has organisation-wide impact. Specifically, few organisations will allow lawyers or legal functions to run privacy – and for good reason; it will become accepted that it is less about complying with the law, and more about running a business in accordance with the fundamental principles of safe privacy operations, which happen to have been embodied within legislation. The lawyers may be called when things go wrong, but as is the case with health & safety, they won't be called to design, implement, and oversee privacy systems and practices.

A final thought

The experiential insights provided by the highly mature safety industry, represent an opportunity to transfer knowledge, skills and solutions from what is, in effect, one systemic operational framework to what will be another. Organisations and privacy professionals should take a long, hard look at how health & safety practices have been adopted and managed, and look to them for inspiration, guidance and, some certainty as to how things might look in the future.

Léon Atkins is Co-Founder and CEO, Europe of Impact Privacy, a solicitor (England & Wales, Ireland), as well as a compliance professional and qualified health & safety practitioner. He has extensive experience in advising on, designing, and managing privacy compliance.


Leon.atkins@impactprivacy.com


+353 (0)1 554 1189


@atkins_leon


www.impactprivacy.com