Compliance
in the Time of a Pandemic

by Hugh Jones

As we approach the first anniversary of the Covid-19 pandemic (remember the heady days of pre-Covid travel, socialising, shopping, etc.?), we are running out of superlatives and descriptions to take account of the singular impact the virus has had on our lives.

Extra-ordinary, worrying, devastating, insidious, sinister, once-in-a-generation event, a 'perfect storm'. None of them do justice to the upheaval and upset we are experiencing, worried for our own and our family members' health, employment, business survival, milestone events like weddings, family gatherings, festivals and conferences. All turned on their head.

Data Protection compliance must appear well down the list of priorities for those who are struggling with the real threat of personal illness, unemployment, business failure, extended school closures, cancelled state exams and concern for elderly or vulnerable family members. And so it should.

There are more than enough sources of information available providing guidance on good practice for handwashing, social distancing and voluntary self-isolation. There is no need to repeat that guidance here, and I won't. However, if an anniversary re-cap is required, we recommend:

The HSE's Health Protection Surveillance Centre:

https://www.hpsc.ie/a-z/respiratory/coronavirus/novelcoronavirus/ and, naturally,

The Data Protection Commission (DPC) regarding general data management:

Data Protection and COVID-19 | 06/03/2020 | Data Protection Commission and

DPC Guidance with regard to working from home:

https://dataprotection.ie/en/protecting-personal-data-when-working-remotely-0

But despite the difficulties posed by these extra-ordinary times, life goes on. Indeed, the very principles on which the GDPR is based act as a quick-reference guide for the kind of habits and behaviours we have had to adopt in recent months.

Improvise, Adapt, Overcome

At a time when we might have been inclined to set all structures aside in the interests of survival, we were encouraged to adopt a reasonable and measured approach to this crisis – consider the privacy and concerns of others, no need for excessive or dramatic responses, no requirement for unnecessary or pointless measures.

It is a measure of current technology that with relatively little disruption, most service sectors have been able to transition to a wholly or predominantly online model quite quickly. With all due respect to the retail, entertainment and cultural sectors which have been so heavily impacted, the ability of a sizeable proportion of the workforce to continue working away from their traditional workplace provided some level of stability, sanity and continuity at a time when long-established models of work were falling apart.

But the transition to working from home brought its challenges.

It is not a new area, as self-employed individuals have been doing so for years, but the sheer volume of workers dispatched to their kitchen tables in such a short period of time was unprecedented. These temporary and interim working environments were less secure, less discrete, lacked supportive colleagues, lacked file storage facilities, are occasionally vulnerable to interruption and intrusion, etc. The cyber-security industry noted a substantial and sudden increase in scams, hacking and ransomware attacks on this home-working population. Traditional governance and monitoring models were also challenged. How to ensure security, but also to measure productivity, attendance, compliance or contribution to the 'bottom line' when the team is dispersed, out of sight if not out of mind?

Organisations have had to exercise discipline and constraint in avoiding the temptation to 'hoover up' additional information that might be available from other sources, however – social media activity, vehicle trackers, 'always on' video-cams and mandatory Zoom calls simply to verify that everyone was up, dressed, working, engaged in the 'day job'.

Added to this, all indications point to the adoption of a form of 'working from home' even after normal service is resumed and employees can once more commute, interact and travel. So, the measures, policies and protocols being refined and adapted during the past months are likely to become a longer-term fixture in our day-to-day activities and policies.

With approximately one in three employees in the UK, Ireland and the US now working exclusively from home, it is sobering to note from recent reports that fewer than one in five has received any form of training on cyber-security or prevention of ransomware or phishing attacks.

As a further indication of the issues confronting employers, over 65% of staff surveyed admitted that where they print work-related material at home, they simply discard the material in the household rubbish bin when it is no longer needed – shredding is not an option available to them at home. The dividend of this is that we are likely to see a steady increase in data breaches in the coming months.

Further, the enforced absence from the workplace means that stored files are less accessible, leading to a substantial delay in responding to requests for individual Data Subject rights. Even where the 60-day extension is available, many organisations have failed to meet their response obligations, leading to further ire among their customers or subscribers.

Many organisations were simply overwhelmed by the rush to dispatch staff to their 'home office' in the early stages of the pandemic and are only recently playing catch up by issuing company devices such as secure laptops, phones and VPN access. In the interim, much correspondence was conducted from personal e-mail or social media accounts using home computers which have nothing like the same security controls and protections as a work device.

From a GDPR perspective, the old adage continues to apply: "Just because you can does not mean that you should". The Regulation requires compliance with principles of proportionality and necessity, resisting the deployment of certain technology on the grounds that it is unnecessarily intrusive and excessive in the personal data being captured, even while the software can be deployed relatively inexpensively and easily.

In other words, just because data is technically available does not mean that its use is lawful or permissible. The compliance challenge has been an additional burden over the past few months. Not only is the employer eager to protect the security and integrity of the data and ensure that business continues to be done, but the eagerly-awaited opportunity for staff to return to the workplace introduced a further set of dilemmas.

As staff began to return to their workplace, employers were naturally concerned for their welfare as well as that of their colleagues. Questionnaires were drafted, criteria were set, Government guidelines were issued and, as ever, more and more data was gathered, reviewed, analysed and stored. With the best of intentions, employers were again exceeding their remit, seeking information on temperature, symptoms, the health of family members, close contacts and facial scans.

Here again, the criteria of necessity and proportionality were most helpful – what is an adequate level of information to be able to decide on a colleague's return to work, and what responses would be a sufficient indicator of risk to merit self-quarantine and enforced isolation.

The GDPR is the employer's friend

Throughout all of these challenges, the GDPR has served to offer accessible, practical criteria against which key decisions can be made.

Principle 1: Obligations of fairness and transparency required employers to provide clear, visible notice with regard to changes in work practices, adoption of extra-ordinary policies to accommodate working from home, explanation of Government guidance in relation to furlough, pandemic payments, suspension of business, capture of health information and, in many cases, disclosure of such data for contact tracing and occupational health.

Principle 2: Specified Purpose and Principle 3: Minimisation enabled organisations to find an appropriate justification for the processing of personal data during these unusual times and (equally importantly) knowing where to draw the line and avoid excessive data gathering and breaches of privacy.

Principle 4: Accuracy drives organisations to consider the level and quality of data required for the various purposes to which it is used, as well as the mechanisms being used to gather the data in the first place. It also provided a timely defence against the plethora of 'snake-oil' peddlers who came out of the woodwork, offering all manner of improbable (and unlawful) solutions to gather staff data, often without their knowledge. GPS trackers, key-stroke monitors, remote camera deployment and facial temperature scanners were all promoted at one time or another, offering dubious claims of new technology and innovation but mostly proving unreliable and inaccurate.

Principle 5: Retention will challenge organisations to consider how long they can lawfully retain information in relation to an employee's or visitor's Covid19 questionnaire responses – the Regulation says 'only for as long as necessary' – here again, the disciplined response will be to delete and remove the data as soon as its health and employee welfare purposes have been served.

Principle 6: Security and Integrity has been the big talking point throughout the pandemic – coming to terms with the changes in circumstances during the 'working from home' phase, minimising the risk by reducing the volume of data in circulation, educating staff to consider their surroundings, manage the data appropriately, exercise caution when conducting confidential client meetings at the kitchen table where housemates might be listening in, etc.

Throughout all of this, the obligations of **Principle 7: Accountability and Responsibility** have not gone away, nor have they been suspended. Despite all of the distractions and upset, life and law have continued their march – we have had the Brexit transition, the Schrems II decision of the Court of Justice of the European Union (CJEU), the de-commissioning of Privacy Shield, the Brexit tension and the six-month Brexit extension (not to mention the odd election, attempted coup and cancelled Olympics).

Compliance with other legislation

Data Protection is not the only regulation being called into play these days – many other obligations and responsibilities apply – employment law, health and safety considerations, contract responsibilities with regard to service delivery and force majeure, social welfare, labour relations and equality legislation will all come under scrutiny as we continue to react and respond to the many difficulties posed by this insidious, spiky disrupter.

And yet it is these rules and obligations which will give us the standards, the measure and the lawful basis on which to make the decisions we need to make at a time when normality has been turned on its head.

Where possible, staff working from home should be advised about the appropriate number to call for IT or Data Protection support, particularly where they feel a breach may have occurred or that they may have been subject to a phishing or ransomware attack.

Employers should seek out online training which colleagues can complete from the comfort of home, raising awareness about security, data governance, recognition of unlawful scams, data management best practice and appropriate disposal of paper and electronic records. Some practical training regarding the domestic working environment and the appropriate tools to use for video conferencing, etc., will also go a long way towards protecting the organisation's interests.

Lastly, this crisis has presented an ever-changing landscape about which we are learning daily – we can only encourage people to heed responsible sources of news and healthcare, and to follow the guidance issued in the best interests of us all.

If we can be of any further support or assistance, please don't hesitate to contact Privacy Engine (formerly Sytorus) at info@PrivacyEngine.io.

Hugh Jones
Founder

Hugh Jones is a founder of Sytorus/ Privacy Engine and a senior DP consultant with experience in the Irish, UK and international privacy sector.