ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Binding Corporate Rules and Brexit – a practical way forward

Sian Rudgard of Hogan Lovells explains what the situation is for organisations that are considering applying for, or already have BCRs approved.

At the end of July, and so with only five months remaining until the end of the transition period, the European Data Protection Board (EDPB) issued an information note for companies that have the ICO as their lead authority as to the steps that they need to take in order to move their Binding Corporate Rules (BCR) application, or approved BCR, to an European

Continued on p.3

Gamify it! Making your data protection training stick

Using games to deliver DP training can be a fun and cost effective way to get your message through. By **Abigail Dubiniecki**, freelance data privacy lawyer and consultant.

Among the many DPO tasks, addressing the human factor is perhaps the most challenging. Effective training can transform an organisation's weakest link into its greatest asset. Yet compliance training is often met with eye rolls by staff, while senior managers see it as a necessary "one-and-done" evil. The result: managers chase employees, employees reluctantly comply, and DPOs continue to hand-hold or

Continued on p.5

New PL&B resources

- PL&B's Data Protection Clinic: Book a 30 minute consultation to help resolve your Data Protection issues. The clinic will support you in identifying your key priorities and much more.

www.privacylaws.com/clinic

- PL&B's *Privacy Paths* podcasts are available at www.privacylaws.com/podcasts and from podcast directories, including Apple, Alexa, Spotify, Sticher and Buzzsprout. Upcoming topics include the impact of the EU-US Privacy Shield's invalidation in the US

Issue 111 **SEPTEMBER 2020**

UNITED KINGDOM
report

ISSUE NO 111 **SEPTEMBER 2020**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS

Sian Rudgard
Hogan Lovells International LLP

Abigail Dubiniecki
Freelance data privacy lawyer

Edwin Baker, Alexander Dittel and Marta Dunphy-Moriel
Kemp Little LLP

Kathleen Morrison
Brodies LLP

Victoria Hordern
Bates Wells

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2047-1479

comment

Can the UK still get EU adequacy?

As the Brexit negotiations are in jeopardy due to the government's new Internal Market Bill, progress made on data protection and UK adequacy may also be hampered. If we end up with a no-deal, Standard Contractual Clauses (SCCs) will play a more significant role in international data transfers. But there are now new challenges caused by the *Schrems II* decision, also in relation to cloud computing (p.11).

The European Commission is currently working on a revised set of SCCs to take the judgment of the Court of Justice of the European Union into account. The European Commission says that this is a top priority for the coming months, with a view to finalising the clauses by the end of this year. Also, discussions have started with the United States to find a way forward. In the UK, the government's National Data Strategy seeks innovative mechanisms for international data transfers (p.9).

There is more certainty over the role of Binding Corporate Rules and changes to the ICO's remit after Brexit. Read our correspondent's analysis and practical advice on p.1.

The Appropriate Design Code is now in effect, and organisations have until 2 September 2021 to ensure compliance. The Code requires high privacy settings as a default. The ICO is issuing guidance and will host webinars on this topic (p.10). It is also keen to have submissions for its Sandbox programme on projects that deal with children's data.

For those who have responsibility for delivering data protection training, this issue brings a wealth of ideas on how to engage staff through data protection themed games (p.1). The aim is to make learning fun and encourage discussion on privacy issues.

The pandemic has changed the working life for many of us. DPOs are now often taking video calls and attending or organising online conferences and meetings. Which data protection rules do we have to keep in mind in this environment (p.17)? And which details are actually included in the broadly defined concept of health data (p.14)? The Information Commissioner responds to MPs' unease about privacy and Covid-19 (p.18) whilst seeing a massive impact on resources due to Covid-related work.

Last but not least, is cookie audit automation your get out of jail card? Find out on p.19 how technology can help the busy DPO.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Gamify!... from p.1

clean up after teams that have disregarded or misconstrued data protection requirements.

With laws like the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and Brazil's General Data Protection Law (LGPD) raising the stakes, getting training right is mission-critical. High completion rates and deep engagement are essential for training to stick.[1] Gamification may help.[2]

What is Gamification?

Gamification uses game design principles to create a fun, play-focused way to learn, using competition or collaboration, points, leader-boards, rewards or missions. Card games, board games, immersive training, quizzes, and more, whether physical or electronic, hi-tech or low-tech, played alone or in teams, together or remotely, have all been used in gamified learning. It's a subset of "Serious Games" because it's main goal is not entertainment, but education.[3]

Why Gamify?

The key driver is motivation. However, there are other objectives as well. Learning happens on a continuum. At a minimum, all staff must know, understand and be able to apply basic data protection concepts at work. But data protection is contextual, and a higher level of learning and skill is required for any situation where a DPO might answer "it depends".[4]

Motivation: Steve Brett co-founded E3 Compliance Training Ltd. with a mission to "rid the world of boring e-learning" by harnessing the power of mobile games to offer a new paradigm for compliance training with enjoyable games that are "part banking app, part Candy Crush." E3's GDPR training[5] is designed for staff, and consists of nine mini-games that deliver short, animated content modules on specific topics followed by rapid-fire quizzes, scenarios and simulations to test players' understanding. Employees get points and rewards for correct answers and can measure their success using leader-boards. Explanations are immediately provided for wrong answers and reinforced later from a different angle. Players can replay games to refresh their memories or improve their scores. The games are designed to appeal to all learning styles.[6] Brett notes: "We certainly see (and get feedback from compliance teams) that using our courses changes the nature of the conversation in the office. Instead of the groans, we get teams talking about the topic in a positive way from what score they got to specifics on the questions."

Some 80 to 95% of employees complete the GDPR training without being chased, and over half repeat it. It takes 40 minutes to complete all nine mini-games, but games are self-paced. The content is highly customisable and clients have even collaborated on bespoke content. E3 clients range from microenterprises to large multinationals in a range of sectors, and the training is suitable for a range of roles and seniority levels.

Communicate and reinforce difficult concepts: Games can also help communicate difficult concepts. Strategic Privacy by Design, the Game by Enterprivacy Consulting Group,[7] is a card game designed to reinforce the concepts in Jason Cronk's Strategic Privacy by Design methodology. Players, who take on different roles, are tasked with identifying and eliminating privacy violations from their product before it's released to the public. Once the product is released, violations earn consequences. The game can be played competitively or cooperatively and is suitable for everyone from web

developers with limited privacy knowledge to seasoned privacy professionals adept at playing strategically. It can be combined with other Enterprivacy resources: infographics, the Privacy Wiki, and the book.[8]

Experiential Learning: Gamification has many other benefits. Kartic Vaidyanathan, founder of Let Us Play to Learn, says games give players the "courage to fail" without judgment. Mistakes are an opportunity to clarify misconceptions, provide immediate feedback, assess trouble spots and spark discussion.[9] Games spark creativity, by providing a realistic scenario to test new ideas without fear of consequences.[10]

WiCompli is a "game-based data protection learning tool" developed by Nyela IG Consultants Ltd in partnership with AKD Solutions Ltd.[11] It's the brainchild of Nyela IG Consultants' founder, Nailah Ukaidi. With over two decades of data protection experience, she realised the GDPR would require more than traditional "talking heads" training: "[The] GDPR introduced a number of developments and signalled a sea change in data protection. … WiCompli brings data protection training into the 21st century but retains an approach that is collaborative, stimulates conversation and collective organisational learning that sticks."

While fun is a key element, WiCompli is a Serious Game in that it aims to educate:

"Our mantra is [that] people learn better when they are having fun. The process is experiential and that's what really makes the difference when it comes to learning and applying what has been learnt to your day to day work."

The tool comes with two animated education pieces (beginner or advanced); a Monopoly-style board game / Learning Map; a facilitator manual and an assessment. Facilitators must have strong data protection knowledge and be trained and licensed to deliver the training in-house. Alternatively, Nyela IG Consultants can deliver the training on-site or virtually.

Questions vary from fact-based ones such as "name three other lawful bases other than Consent" to scenario questions that provoke deeper analysis, such as "You return from the office and realise you have left a client file at their home. What's the issue and what would you do?" This helps address the more nuanced and contextual dimensions of data protection in a way that right/wrong questions cannot do, and pushes players to higher-order thinking.

There are also "Opportunities" and "Threats" cards, which highlight strengths and weaknesses that exist and how these are achieved and addressed. A player might draw a "You forgot to do a DPIA for your automated facial recognition CCTV project. Lose 500 points" or "Your use of Consent is found to be valid – fully informed, specific, freely given, intelligible and easily accessible. Gain 750 points." These set the scene for deeper discussion and action planning.

Finally, there are "Enforcement/ Regulator" cards which remind players about the pitfalls and risks associated with non-compliance which are much wider than personal data breaches.

The tool is highly flexible and customisable and caters to a wide audience. It can be used to train staff in a range of roles and at varying levels of data protection expertise and can be played in as little as two hours or for a full day. The role of the trained facilitator is critical. The facilitator sets the learning objectives, selects the appropriate content (from a wide selection of cards), facilitates discussion, answers questions and notes trouble areas. For example, the facilitator may decide to do a deep dive on Consent or Data Processors or use it to draft a Privacy Notice or respond to a simulated data breach. WiCompli's updated content cards address new developments, like Brexit, and clients can also request customised terminology and card content that is specifically tailored to the industry, organisational purpose and culture, including the business logo.

Games spark creativity, by providing a realistic scenario to test new ideas without fear of consequences.

WiCompli clients come from various industries and sizes, from microenterprises to large multinationals, schools and colleges, housing associations, national utilities and financial institutions. Clients include Scottish Water, Gamesys Group, Afreximbank and the London School of Economics and Political Science.

Learning by Doing: LINDDUN GO is a gamified version of LINDDUN,[12] a privacy threat modelling methodology that was designed to bridge the chasm between lawyers, DPOs and engineers by providing a model for systematically eliciting and addressing privacy threats in software architectures. LINDDUN is a recognised Privacy Engineering methodology in ISO 27550.[13]

As Kim Wuyts, Post-Doctoral Researcher at DistriNet, KU Leuven explains, she and her co-creators created LINDDUN GO to offer a "lightweight privacy threat modelling approach that is easy to apply, without overhead or friction, and that has a low threshold, making it suitable for people who are relatively new to the privacy field, while keeping a high level of thoroughness and traceability."

Inspired by the Elevation of Privilege game[14] by Adam Shostack (which gamifies Microsoft's STRIDE security threat modeling approach), players identify different types of privacy threats and mitigations in a data flow map using handy playing cards as prompts.

While intended as a support privacy engineering at the design stage, it helps all participants learn by doing in a collaborative way, confidently brainstorming different solutions. This makes it particularly suited to agile / DevOps organisations[15] that don't have the luxury of wading through extensive documentation. The full game can be downloaded for free from their website.[16] It pairs well with Elevation of Privilege.[17] Shostack lists a host of other gamified cybersecurity games on his website worth considering.[18]

Avoiding table-top pitfalls: Tabletop exercises, while helpful, are prone

to pitfalls such as incomplete or highly unlikely "what-if" scenarios. Blackhills Information Security created breach incident response card game "Backdoors and Breaches" as a gamified alternative.[19] It's modelled after Dungeons and Dragons and is designed to get players to identify technical and procedural vulnerabilities an attacker might exploit. Similarly, academics in Germany have created and tested a Serious Game that elicits social engineering threats in the workplace.[20] Many cybersecurity games challenge players to think like hackers, such as Clearview Data Management's Immersive Cybersecurity Training,[21] which is being adapted for virtual delivery.

As with WiCompli, adept facilitation is key, since sparking discussion is an important part of the game. In addition to identifying vulnerabilities, employees start to explore solutions and apply them to their own work environment, so it has the double benefit of trouble-shooting real-world issues within the organisation.

Does it work?

It depends. If the aim is to motivate staff to complete training, gamification will generally be effective.[22] But what is "effective" will depend on the learning objective.[23] If it's to raise general awareness to a beginner audience, testing their knowledge with right/wrong answers may suffice. But if it's to elicit deeper discussion and prepare staff to successfully implement Data Protection by Design, key metrics on operational outcomes coupled with qualitative and anecdotal data may be more appropriate.

E3 prides itself on its data-driven approach. E3 generates insights by analysing performance data and on several occasions have helped clients identify areas of risk associated with unmet learning objectives. The DPO can then act on this information to provide additional support. E3 is a processor and worked to design the mobile game with Privacy by Design in mind.

WiCompli also encourages participants to take what they have learnt back to the workplace and Nyela IG Consultants report receiving consistent feedback from clients on the real difference that WiCompli makes to staff understanding and application of data protection.

Industry professionals and students who have tried LINDDUN GO have reported it is easier to use than LINDDUN, and they appreciate the collaborative approach, which provokes discussion within interdisciplinary teams.

How can I bring gamification into my training?

1. Define your learning objectives[24] and tailor content to players' needs.
2. Choose your game(s) or create your own.[25] But remember: employees are Data Subjects too. Assess possible data protection impacts, consider ethical issues and keep it within the workday. Avoid "mandating fun", as it could backfire.[26]
3. Use them wisely: The game is a tool and its effectiveness will vary with use and your objectives. Glenn Mills of Cover Compliance LLC cautions that too much focus on competition or entertainment can cause players to miss the subtleties and substance of training.
4. Use it often: training and policies need to be reinforced. Mills encourages clients to use gamification throughout the year to keep data protection top of mind.
5. Learn from your learners: Employees may identify vulnerabilities you hadn't considered and propose creative, practical solutions during gamified training. Make them allies, not mere subjects, and take notes.
6. Measure effectiveness according to your objectives, using both quantitative and qualitative data.

Conclusion

Gamification has the potential to increase employee motivation and engagement, resulting in better learning outcomes. So does it work? As we often say in data protection: 'It depends'. It is one of many tools in the DPO toolbox. Its effectiveness will depend on how you use it.

AUTHOR

Abigail Dubiniecki is a freelance data privacy lawyer and consultant.
Email: LegallyAbigail@protonmail.com

REFERENCES

1 Baxter, Ryan J. and Holderness, Darin Kip and Wood, David A., Applying Basic Gamification Techniques to IT Compliance Training: Evidence from the Lab and Field (October 21, 2015). Available at SSRN: ssrn.com/abstract=2517022

2 See e.g. Silic, Mario and Lowry, Paul Benjamin, Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance (January 1, 2020). *Journal of Management Information Systems* (JMIS), vol. 37(1), pp. 129-161, Available at SSRN: ssrn.com/abstract=3431995 at p. 3.

3 Baxter, *et al*., *supra* n. 1 at p. 6.

4 The 2001 Revised Taxonomy of Educational Objectives, an update of Bloom's Taxonomy lists six cognitive processes along a continuum: Remember; Understand; Apply; Analyze; Evaluate; Create. Knowledge (factual, procedural or conceptual) is a pre-condition for each. See https://cft.vanderbilt.edu/2010/04/bloom s-revised-taxonomy-a-framework-for-assessing-student-learning

5 www.e3ct.com

6 www.e3ct.com/news/2017/7/19/7-learning-styles-and-gamification

7 privacybydesign.training/game-play/

8 privacybydesign.training/learning-tools/

9 "Inspiring Ideas Podcast" interview: anchor.fm/inspiringideas/episodes/Kartic-Vaidyanathan—-Re-imagining-corporate-learning-through-power-of-play-eibrrm/a-a300t66

REFERENCES

10 K. Beckers and S. Pape, "A Serious Game for Eliciting Social Engineering Security Requirements," 2016 IEEE 24th International Requirements Engineering Conference (RE), Beijing, 2016, pp. 16-25, online : ieeexplore.ieee.org/document/7765507 at p.3.

11 WiCompli: www.igconsultants.org/wicompli/ AKD Solutions Ltd.: www.akdsolutions.com/

12 www.linddun.org .

13 www.iso.org/obp/ui/#iso:std:iso-iec:tr:27550:ed-1:v1:en

14 www.microsoft.com/en-us/download/details.aspx?id=20303

15 Agile is an equal opportunity team: every member of the scrum can do every job within the team, which prevents slowdowns and bottlenecks. DevOps, on the other hand, assumes separate teams for development and operations, and people stay within their teams, but they all communicate frequently. www.bmc.com/blogs/devops-vs-agile-whats-the-difference-and-how-are-they-related/#:~:text=Specialization.,but%20they%20all%20communicate%20frequently

16 LINDDUN.ORG/GO. See also Kim Wuyt's paper lirias.kuleuven.be/3056246 available in late Fall, and her IWPE presentation youtu.be/hWpZ-CozRBs

17 There are two privacy extensions but they are not as in-depth as LINDDUN. STRIPED: logmeincdn.azureedge.net/legal/gdpr-v2/eop-cards-ready-to-print.pdf) and STRIDE+TRIM: github.com/F-Secure/elevation-of-privacy

18 adam.shostack.org/games.html

19 www.blackhillsinfosec.com/projects/backdoorsandbreaches

20 See Beckers, *et al*, supra note 11.

21 vimeo.com/343208448 See also Adam Shostack's extensive list of table-top games: adam.shostack.org/games.html

22 All the studies cited in this article noted motivation improved with gamification.

23 Refer to the 2001 Revised Bloom's Taxonomy mentioned earlier, *supra* note 4.

24 See the 2001 Revised Bloom's Taxonomy, *supra* note 4.

25 Create a table-top game on Gamecrafter: www.thegamecrafter.com/ or an electronic quiz on Kahoot kahoot.com/business/

26 See Mollick, Ethan R. and Rothbard, Nancy, Mandatory Fun: Consent, Gamification and the Impact of Games at Work (September 30, 2014). *The Wharton School Research Paper Series*, Available at SSRN: ssrn.com/abstract=2277103 or dx.doi.org/10.2139/ssrn.2277103

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access UK events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

"I've always found *PL&B* to be a great resource for updates on privacy law issues, particularly those with a pan-EU focus. It strikes the right balance for those in-house and in private practice. The content is clear, well presented and topical."

Matthew Holman, Principal, EMW Law LLP

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 33rd year. Comprehensive global news, currently on 165+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.