**The importance of keeping your company’s trade secrets, secret**

**Andrew Beale\* and Jane Foulser McFarlane\*\***

*Risk Management, Intellectual Property, Trade Secrets, Cyber security*

**Abstract**

This article offers a legal analysis of the future operation of the UK Trade Secrets (Enforcement, etc.) Regulations 2018 and how risk management training about these Regulations will assist Company Boards of Directors and Senior Managers to better understand and protect their firms’ intellectual property.

\* OBE, Associate Professor, Director of IP Wales and Member of the International Institute of Shipping and Trade Law (IISTL) - *address for correspondence a.j.beale@swansea.ac.uk*

\*\* Barrister, 30 Park Place Cardiff and 3PB

The authors express their thanks and appreciation to Professor Andrew Tettenborn (Member IISTL) for his comments on the working draft, any errors herein remain those of the authors.

**Introduction**

Corporate awareness of intellectual assets is now at a level where they can no longer be perceived as being the “hidden assets” of a company. The next big challenge is to recognise and respond to online threats to these intellectual assets.[[1]](#footnote-1) Research undertaken by IP Wales on behalf of the Welsh Government found small to medium sized enterprises (SMEs) to be particularly vulnerable to cyberattacks, with many taking little or no precautions against cyber threats in the mistaken belief that they were too small to attract the cybercriminal’s attention, or that they did not possess any data worth stealing.[[2]](#footnote-2)

This is not true today. In the digital era, data is the prize for cybercriminals and any data which is of value to any company is a worthwhile target for them. Such data may include any of the following: technical & scientific information (especially know-how); commercial information (especially customer profiles); and financial information (such as customer credit card details). Even negative data can have commercial value: for instance, research projects which have culminated in a dead end or failed manufacturing processes.

Governments are increasingly coming to follow the policy lead from the USA and recognise that, “trade secrets may constitute the ***most*** critical intellectual assets…effective protection of trade secrets is especially important for mSMEs, which may be disproportionately affected by and less able to recover from a misappropriation compared to larger enterprises.”[[3]](#footnote-3)

In *the Protection of Data in our Digital Age [[4]](#footnote-4)* one of the present authors noted as follows:

 “[I]n large measure the existing legal protection of trade secrets data is limited due to a low level of legal protection,[[5]](#footnote-5) issues of legal fragmentation both across and within differing legal jurisdictions around the world and problems associated with poor civil redress and criminal enforcement, including a failure to protect the confidentiality of trade secrets during legal proceedings. Difficulties in finding an agreed understanding of ‘trade secrets’ and ‘know-how’ resulted in TRIPS[[6]](#footnote-6) adopting the more neutral term ‘undisclosed information’, whilst at the same time refusing to offer any legal definition as to its meaning. In consequence, a recent study by the World Trade Organisation has found that legal protection of confidential information in member states today derives from over 25 different fields of law.[[7]](#footnote-7) Moreover, TRIPS was negotiated at a time when the usage and storage of digital data was in its infancy, a global economy underpinned by employee mobility was still in creation and the notion of globally dispersed research and development driven by what was to become known as ‘open innovation’ remained still to be discovered by the boards of most large multi-national corporations.”

In attempting to address this deficit in the legal protection of trade secret data the EU Commission introduced Directive 2016/943 *on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure* (henceforth the EU Directive). This Directive was brought into force within the UK by the Trade Secrets (Enforcement, etc.) Regulations 2018[[8]](#footnote-8) [henceforth the new Regulations], which for the first time has enshrined into UK law a new statutory definition for a “trade secret”: namely, as data which -

*“(a) is* ***secret*** *in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question,*

*(b) has* ***commercial value*** *because it is secret, and*

*(c) has been subject to* ***reasonable steps under the circumstances****, by the person lawfully in control of the information, to keep it secret…”[[9]](#footnote-9)*

A number of these terms could do with elucidation.

**“Secret”**

The preamble to the EU Directive, on which the new Regulations are based, makes clear that its definition “excludes trivial information and the experience and skills gained by employees in the normal course of their employment, and also excludes information which is generally known among, or is readily accessible to, persons within the circles that normally deal with the kind of information in question.”[[10]](#footnote-10) Such an interpretation does not, however, restrict the use of “reverse engineering”[[11]](#footnote-11) as a legitimate means to obtain access to trade secret data.[[12]](#footnote-12)

**“Commercial value”**

The preamble to the EU Directive additionally states that data has a commercial value “where its unlawful acquisition, use or disclosure is likely to harm the interests of the person lawfully controlling it, in that it undermines that person's scientific and technical potential, business or financial interests, strategic positions or ability to compete.”[[13]](#footnote-13) The minimum threshold for recognition will thus be, in essence, “the extent to which the information provides an opportunity to obtain an advantage over competitors who do not know or use it.”[[14]](#footnote-14)

**“Reasonable steps under the circumstances”**

There is no definitive guidance yet under UK law as to what might be the interpretation of “reasonable steps”, or for that matter “under the circumstances”. On the other hand, there may well be indications elsewhere. Our courts may be well advised to turn to jurisprudence from the USA, given the EU Directive mirrors Article 39.2 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs), which of itself took inspiration from the American Uniform Trade Secrets Act, as widely adopted by individual states across the USA.[[15]](#footnote-15) So what lessons might the UK Company Lawyer glean from U.S. case law on the likely interpretation of “reasonable steps under the circumstances” under these new Regulations?

1. ***Review your company’s data estate***

U.S. courts have found it problematic if the claimant has done “nothing to differentiate its protective measures for the alleged proprietary trade secrets from those imposed on any other corporate information.”[[16]](#footnote-16) The court found it problematic that there was no allegation that the plaintiff treated the alleged trade secret as “any more confidential than all of the plaintiff’s internal information.”[[17]](#footnote-17)

1. ***Your company’s trade secrets should be identified as such***

U.S. courts have considered the labelling of information as “Confidential”, or “Trade Secrets” as a factor in the determination of whether that status was deserved*.*[[18]](#footnote-18) An interesting situation can be seen in *Call One Inc v Anzine*,[[19]](#footnote-19) a Federal claim, which was summarily dismissed on the basis that although the plaintiff had a policy in place requiring all confidential and trade secret information to be labelled as such, the stolen information was not actually labelled as such, the court finding that no reasonable jury could conclude that the defendant therefore had a duty to maintain the secrecy of that information.

U.S. Courts have also determined the loss of trade secret status when data was disclosed without the markings required under a confidentiality agreement.[[20]](#footnote-20)

1. ***Use Non-Disclosure Agreements***

What the U.S. cases indicate is making employees,[[21]](#footnote-21) and anyone else the secret is revealed to,[[22]](#footnote-22) subject to a confidentiality agreement is merely a starting point. Without more, a claim for trade secret protection is likely to fail.[[23]](#footnote-23) This is even more likely where the only step taken is a non-competitive covenant which is found to be unenforceable, which was the situation in *Arcor v Haas*.[[24]](#footnote-24) Measures that go beyond normal business practices may be required, such as demonstrating that employees understood that the data was to be kept confidential.[[25]](#footnote-25)

Reliance upon luck, rather than judgment, proved fatal to trade secret protection for the plaintiff in *CMBB LLC v Lockwood Mfg.*[[26]](#footnote-26) The court granted summary judgment in favour of the defendant, stating that the plaintiff had “appeared to rely upon luck and a somewhat naïve faith in its employee-employer good will, rather than taking the necessary affirmative and calculated steps to safeguard what it now characterises as valuable and secret information.”

1. ***Be mindful of the employment situation***

An analysis of trade secrets cases within the USA has revealed that in nine out of ten cases, at both the state and federal levels, the defendant was either an employee, former employee or otherwise a business partner.[[27]](#footnote-27)

One of the primary ways of revealing trade secrets to a competitor, is through employee misconduct, when they intentionally; unintentionally; or negligently misappropriate information. To combat this and to satisfy the requirement of “reasonable steps”, employers should limit access on a need-to-know basis; restrict ex-employee access; and institute a comprehensive system of employee education.

In *Stampede Tool Warehouse Inc. v May*[[28]](#footnote-28) limited customer information was given to employees on a strict need-to-know basis. In addition, offices were kept locked; the garbage was checked daily; employees had special computer access codes; hard copies of customer lists, customer cards and call books used by the sales staff were kept under lock and key; security cameras were in place; and NDA’s were signed, which stated that the names of the customers could not be used or disclosed because they were the property of the plaintiff and were confidential. Not surprisingly, the court granted trade secret protection.

The time when employees leave a company is a high-risk situation for trade secrets theft. Recognising this fact, U.S. courts have noted the failure of a company to cut-off an ex-employee’s access to data, as supporting a finding that insufficient reasonable steps had been taken. In *Orthofix Inc. v Hunter*[[29]](#footnote-29) this was evidenced by the Plaintiff failing to make any meaningful efforts to seek the return of any trade secret information that the defendant possessed. Similarly, allowing employees to store company information on personal devices and failing to request that this company data was returned on them leaving employment, can be seen as a failure to take reasonable steps.[[30]](#footnote-30)

In *Liebert v Mazur*[[31]](#footnote-31) it was noted that in every case relied upon by the plaintiff, where reasonable steps had been found to have been taken, the trade secrets owner had informed its employees verbally or in writing, about confidentiality.

1. ***Review your IP cybersecurity***

In the USA it has been stated that “it is not necessary that an ‘impenetrable fortress’ be erected to retain legal protection for trade secrets.”[[32]](#footnote-32) However, an analysis of U.S. jurisprudence leaves the reader with a distinct impression that even if an “impenetrable fortress” is not a necessity, and especially perhaps for smaller enterprises, the burden placed upon the party alleging a trade secret is still a surprisingly onerous one.

U.S. courts have assessed the taking of “reasonable steps” in IP cybersecurity to include:- identity and access management (password protection; need-to-know access, secure server storage); data security measures (USB use restrictions, distribution controls); perimeter and network defences (firewalls, data encryption, online use restrictions); communication (pop-up warnings); and email monitoring.[[33]](#footnote-33)

Whilst any steps taken must be reasonable, they need not be any more than that. In *Learning Curve Toys Inc. v Playwood Toys Inc.*[[34]](#footnote-34) the court made clear that whilst it “requires reasonable steps to maintain secrecy, it does not require perfection.”

1. ***Acquiescence is not an option***

The owner of trade secrets must be vigilant in protecting its confidential nature. Poor enforcement of measures may be worse than no protective measures at all. This was evidenced in the case of *Compuware Corp. v Health Care Serv. Corp.*[[35]](#footnote-35) in which it was an undisputed fact that the Plaintiff had known for several months prior to bringing their claim, that the licensee was allowing a third party to use the licensed software, but took no action to prevent this happening, until it became aware that they were using it for an unapproved purpose. The court determined such inactivity was critical to its trade secrets claim, “[A]s a matter of law, doing nothing to enforce a confidentiality agreement is not a reasonable effort….to maintain a trade secret.”[[36]](#footnote-36)

1. ***Size does matter***

There has been much speculation that “under the circumstances” will allow for a more favourable treatment of SMEs under the new Regulations, via the judicial adoption of a lower benchmark for smaller companies.[[37]](#footnote-37) In *Puroon v Midwest Photographic Res. Ctr. Inc.*[[38]](#footnote-38) a court in the Northern District of Illinois, determined that “reasonable steps for a two or three person operated shop, may be different from reasonable steps for a larger company,” and given the fact that Puroon was a company owned by a single person, a reasonable jury could find that the efforts of its founder and CEO to show physical prototypes of its photo album product to a limited number of potential customers and granting full access to its manufacturing specifications, only after the NDA was signed, were adequate steps to protect the company’s secrets.

Smaller companies are not necessarily expected to take the same expensive steps to protect secrecy as larger ones. In *Elmer v Miller*[[39]](#footnote-39) it was held that a small tailoring shop that kept its customer list in a closed file draw, notified its employees that the list was confidential and limited access on a need-to-know basis, satisfied the reasonable steps requirement. Nevertheless, whilst the “[D]etermination of what steps are reasonably necessary to protect information is different for a large company than for a small one,”[[40]](#footnote-40) a small business is still under an obligation to undertake at least some affirmative measures to protect its confidential information.

1. ***But may not be the only determining factor***

On a cautionary note however, the size of a company need not be the only determining factor. In *Fail-Safe LLC v A.O. Smith Corp.*[[41]](#footnote-41) the court was applying the Wisconsin Uniform Trade Secrets Act and the Seventh Circuit affirmed the grant of a summary judgment because the plaintiff, a small company, had disclosed trade secrets to the defendant while negotiating a joint development agreement, without taking sufficient steps to protect confidentiality. Although the plaintiff had signed the defendant’s NDA, the defendant had not, neither did it give any other promise of confidentiality to the plaintiff. The court stated that although the plaintiff may have been a small company, it was “a sophisticated party familiar with confidentiality agreements” and therefore had acted unreasonably in failing “to take any steps to maintain secrecy.”

**Conclusion**

The driver behind the EU Commission proposing the EU Directive was to position European Companies on a level playing field with their counterparts in the USA and Japan.[[42]](#footnote-42) However, unlike the U.S. Defend Trade Secrets Act[[43]](#footnote-43) the new Regulations offer no criminal sanction against the misappropriation of trade secrets data. Indeed, UK criminal law has traditionally viewed the unauthorised taking of information as a purely civil matter and is unlikely[[44]](#footnote-44) to even consider data as “property”[[45]](#footnote-45) within the meaning of the Theft Act.[[46]](#footnote-46) So the criticism of Lord Boyle that, “it is not too much to say that we live in a country where…the theft of the board room table is punished far more severely than the theft of the board room secrets,”[[47]](#footnote-47) holds as true today as it did more than fifty years ago.

Section 3 of the new Regulations makes clear that the “wider protection” afforded under the common law for a breach of confidence in confidential information still remains in place, with the UK government being of the somewhat limited view that the EU Directive was in any event only a reflection of the existing common law rules, which already provide for the remedies of damages or injunctive relief.[[48]](#footnote-48) Post-employment restraints legitimately imposed on former employees, and technical and business secrets may have already enjoyed protection under our common law, but only to the extent that judicial discretion determined there had been, the necessary quality of confidence; disclosure to the recipient under an express or implied obligation of confidence; and they had been subject to unauthorised use.[[49]](#footnote-49)

Only time will tell the extent to which the UK courts will look across the Atlantic for guidance on the interpretation of “reasonable steps in the circumstances”. But unless and until companies become aware of how high the bar will be set to discharge the legal burden of showing that these measures have been taken, there is likely to be a reluctance on the part of many SMEs in particular to fully utilise the potential benefits[[50]](#footnote-50) of these new Regulations.

The UK is unlikely to differ from the USA insofar as the efforts of the claimant will be evaluated in light of the entire factual situation, with no definitive checklist of applicable precautions to cover all situations available for guidance.[[51]](#footnote-51) However, it will be open to the UK judges to develop a non-exhaustive list of the basic precautions that a trade secrets holder should take, in order to satisfy the requirement of reasonableness, which is likely to become the greatest legal hurdle to overcome under the new Regulations. The most obvious measures will include the restriction of access to information, such as physical or network security; NDA’s; and the marking of documents as “Confidential”. Companies will be required to have in place, a number of components to evidence the existence of an effective Trade Secret Policy. This will necessitate measures to identify, assess and manage trade secret assets and the risk of its misappropriation. It will be reasonable to appoint an individual or team of individuals to develop procedures to implement the Policy, with the starting point being an effective internal and external NDA. Employees should undergo education and training on IP security, and corrective measures should be in place, in order to ensure the consistent enforcement of the Trade Secrets Code of Conduct. The implementation of entry and exit interviews for employees should form part of these reasonable safeguards. Limiting access to certain areas of the premises, along with the issue of ID badges, may seem basic and obvious, but it will be a sensible starting point.

Once the UK courts begin to identify recurring factors which go on to constitute evidence of “reasonable steps in the circumstances”, we might anticipate the growth of specialist trainers, who profess to have detailed knowledge of trade secret protection and who are hired by corporations to undertake an assessment of the measures which have been put in place, and to provide the appropriate training and certification of compliance. This has already been evidenced in the UK, following the implementation of the General Data Protection Regulation (GDPR).[[52]](#footnote-52) With appropriate oversight, such a certification of compliance, may in itself, come to satisfy the requirement of “reasonable steps” in the course of trade secret litigation, but this has yet to be tested in any jurisdiction.

1. IP Commission on the Theft of American Intellectual Property *Review: Progress and Updated Recommendations* February 2019. [↑](#footnote-ref-1)
2. Jane Foulser-Mcfarlane, *Intellectual Property Rights: Infringement and Enforcement Issues in IP Wales funded businesses,* 2011 (on file with the authors). [↑](#footnote-ref-2)
3. Mike Palmedo, APEC Ministers Endorse *Best Practices in Trade Secret Protection and Enforcement Against Misappropriation (infojustice.org, 21 November 2016) <* <http://infojustice.org/archives/37372>> accessed 8th August 2019. *Emphasis added* [↑](#footnote-ref-3)
4. A. Beale, S. Ratcliffe & A. Tettenborn, “The Protection of Data in our Digital Age” [2017] J.B.L, 461, 470. [↑](#footnote-ref-4)
5. R. Jacob, D. Alexander & M. Fisher, *Guidebook to Intellectual Property* (6th edn, Hart 2013) at 205 - “Trade secrets are non-exclusive, so it is not a misappropriation to independently discover the secret information or otherwise reverse engineer it from a properly obtained source. Moreover, trade secrets have been described as ‘too slippery’ for any higher legal protection because information is not treated in law as property.” [↑](#footnote-ref-5)
6. World Trade Organisation, Agreement on Trade-Related Intellectual Property Rights, 1994. [↑](#footnote-ref-6)
7. *Survey on Technology Transfer Agreements and Antitrust* (2013) WIPO Geneva. [↑](#footnote-ref-7)
8. SI 2018/597. [↑](#footnote-ref-8)
9. SI 2018/597, para.2 (*emphasis supplied*). [↑](#footnote-ref-9)
10. Paragraph 14, Directive (EU) 2016/943. [↑](#footnote-ref-10)
11. The retrospective analysis of a product to understand its (hidden) functional aspects and underlying ideas. [↑](#footnote-ref-11)
12. Op. cit. n.5. [↑](#footnote-ref-12)
13. Op. cit. n.10. [↑](#footnote-ref-13)
14. UNCTAD-ICTSD, Resource Book on TRIPS and Development (Cambridge University Press 2005) at 529. [↑](#footnote-ref-14)
15. Ibid, at 521. [↑](#footnote-ref-15)
16. *Opus Fund Servs. (USA) LLC. v Theorem Fund Servs. LLC.*, No. 17-cv-923, 2018, WL 1156246 at 5 (N.D. Ill. Mar 5 2018). [↑](#footnote-ref-16)
17. Ibid, at 6. [↑](#footnote-ref-17)
18. *OTR Wheel Engineering Inc. v West Worldwide Services Inc.*,No. cv-14-085-LRS (E.D. Wash. Nov 30th 2015). [↑](#footnote-ref-18)
19. *Call One v Anzine,* 2018 WL 2735089 (N.D. IL, 2018) at 9. [↑](#footnote-ref-19)
20. *Convolve, Inc. v. Compaq Computer Corp.*, 812 F.3d 1313 (Fed. Cir. 2016). [↑](#footnote-ref-20)
21. *Mintel International Group Ltd v Neergheen* No. 8-cv-3939, 2010 WL 145786 (N.D. Ill. Jan 12 2010). [↑](#footnote-ref-21)
22. *ISC-Bunker Ramo Corp. v Altech, Inc.*,765 F. Supp.1310 (N.D. Ill. 1990). [↑](#footnote-ref-22)
23. *Opus Fund Servs. (USA) LLC. v Theorem Fund Servs. LLC.*, No. 17-cv-923, 2018, WL 1156246 at 5 (N.D. Ill. Mar 5 2018). [↑](#footnote-ref-23)
24. *Arcor Inc. v Haas*, 363, Ill. App. 3d, 396, 402-03, 842, N.E. 2d, 265, 271 (1st Dist. 2005). [↑](#footnote-ref-24)
25. *Gillis Associated Indus Inc. v Cari-All Inc.*,206, Ill. App. 3d 184, 192, 564 N.E. 2d, 881, 886, (1st Dist. 1990). [↑](#footnote-ref-25)
26. *CMBB LLC v Lockwood Mfg Inc.*, 628 F. Supp. 2d 881 (N.D. Ill. 2009). [↑](#footnote-ref-26)
27. Almeling et al. (2010) and (2011), cited in the Report prepared for the EU Commission under contract number MARKT/2011/128D, *Study on Trade Secrets and Confidential Business Information in the Internal Market* (Ref.Ares(2016)98815 – 08/01/2016, April 2013) at 107. [↑](#footnote-ref-27)
28. *Stampede Tool Warehouse Inc. v May,* 272, Ill. App. 3d, 580, 209, Ill. Dec. 281, 651, N.E. 2d. 209 (1995). [↑](#footnote-ref-28)
29. *Orthofix v Hunter,* 55 F. Supp. 3d 1005, 1013 (N.D. Ohio 2014), 630 F. Appx 566 (6th Cir. 2015). [↑](#footnote-ref-29)
30. *Form Factor Inc. v Micro-Probe Inc.*,No. 10-cv-3095, PJH at 11 (N.D. Cal. Jun 7 2012). [↑](#footnote-ref-30)
31. *Liebert Corp. v Mazur,* 357, Ill. App. 3d, 265, 293, Ill. Dec 28, 827 N.E. 2d, 909 (2005). [↑](#footnote-ref-31)
32. *Boston Scientific Corp. v Dongchul Lee*, No. 1:13-cv-13156-DJC (D. Mass.). [↑](#footnote-ref-32)
33. Center for Responsible Enterprise and Trade, *The Importance of Cybersecurity for Trade Secret Protection: Developments in trade secrets cases and the growing role of the NIST Framework* (2016). [↑](#footnote-ref-33)
34. *Learning Curve Toys v Playwood Toys Inc.*, 342 F. 3d, 714, 725, (7th Cir. 2003). [↑](#footnote-ref-34)
35. *Compuware Corp. v Heathcare Serv. Corp.*, 203 F. Supp. 2d, 952 (N.D. Ill. 2002). [↑](#footnote-ref-35)
36. Ibid, at 958. [↑](#footnote-ref-36)
37. J. Hull, “Trade Secrets – reasonable steps*”* [2019] CIPA Journal, Volume 48, Number 10, at 18. [↑](#footnote-ref-37)
38. *Puroon Inc. v Midwest Photographic Res Ctr Inc.*, No.16-cv-7811, 2018, WL 5776334 (N.D. Ill. Nov 22018) at 7. [↑](#footnote-ref-38)
39. *Elmer Miller Inc.* *v Landis,* 253 Ill. App. 3d 129, 134, 625 N.E. 2d, 338, 342 (1st Dist. 1993). [↑](#footnote-ref-39)
40. *Jackson v Hammer,* 274, Ill. App. 3d, 59, 67, 652 N.E. 2d, 809, 815 (4th Dist. 1995). [↑](#footnote-ref-40)
41. *Fail-Safe LLC v A.O. Smith Corp.*,674, F. 3d, 889 (7th Cir. 2012). [↑](#footnote-ref-41)
42. See Commission Response to the Report prepared for the EU Commission contract number MARKT/2011/128D, *Study on Trade Secrets and Confidential Business Information in the Internal Market* (Ref.Ares(2016)98815 – 08/01/2016, April 2013). [↑](#footnote-ref-42)
43. 130 Stat. 376. [↑](#footnote-ref-43)
44. See e.g. Oxford v Moss [1979] 68 Cr App R 183. [↑](#footnote-ref-44)
45. Op. cit. n. 5. [↑](#footnote-ref-45)
46. Section 4(1) Theft Act 1968. [↑](#footnote-ref-46)
47. Hansard (HC) 13 December 1968, vol 775, col 806. [↑](#footnote-ref-47)
48. UK Intellectual Property Office, *Consultation on draft regulations concerning trade secrets*, at 10. [↑](#footnote-ref-48)
49. T. Aplin, L. Bently, P. Johnson & S. Malynicz, *Gurry on Breach of Confidence* (2nd edn. OUP 2012) at 6.06-7. [↑](#footnote-ref-49)
50. See e.g. Explanatory Memorandum to the Trade Secrets (Enforcement etc.) Regulations 2018 No.597 at 11.2. [↑](#footnote-ref-50)
51. *Nordstrom Consulting Inc. v M&S Technologies, Inc.*,No. 06 C 3234, 2008, WL 623660 (N.D. Ill. Mar 4 2008). [↑](#footnote-ref-51)
52. Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (Data Protection Directive) General Data Protection Regulation (EU) 2016/679 (GDPR), 14 April 2016, implemented 25 May 2018 [↑](#footnote-ref-52)