Int. Cybersecur. Law Rev. (2021) 2:339–348
https://doi.org/10.1365/s43439-021-00041-8

Numbers and statistics: data and cyber breaches under the General Data Protection Regulation

Julia Utzerath · Rhea Dennis

Received: 15 September 2021 / Accepted: 16 September 2021 / Published online: 21 October 2021

Abstract Since the General Data Protection Regulation (GDPR) became effective in 2018, enforcement has been at the core of protecting personal data in the European Union (EU). The EU data protection authorities have imposed fines for various types of GDPR breach, and have targeted organisations in multiple sectors, including consumer, technology, media and telecom (TMT), healthcare and industry. The frequency and size of these fines have increased annually, and it is clear that the EU Data Protection Authorities (DPAs) are increasingly cracking down on non-compliance. This article focusses on the fines imposed for breaches of article 32 GDPR, which deals with security of data processing. Article 32 requires organisations to have sufficient technical and organisational measures (TOM) in place to protect them from data breaches, cyber breaches and data security incidents, both internally and externally. As of the end of June 2021, about one fifth of all GDPR fines were imposed for article 32 infringements.

Keywords Cyber security · Internal data breach · External data breach · Technical and organisational measures · Article 32 GDPR

Julia Utzerath
Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB, Feldmühleplatz 1, 40545 Düsseldorf, Germany
E-Mail: julia.utzerath@freshfields.com

Rhea Dennis (✉)
Freshfields Bruckhaus Deringer LLP, One New Bailey, 4 Stanley Street, Salford, M3 5JL, Greater Manchester, UK
E-Mail: rhea.dennis@freshfields.com

Zahlen und Statistiken: Datenschutz- und Cybersicherheitsverletzungen im Rahmen der Datenschutz-Grundverordnung

Zusammenfassung Seit dem Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) im Jahr 2018 haben die europäischen Datenschutzbehörden ihre Untersuchungen und Maßnahmen zur Durchsetzung des Schutzes personenbezogener Daten in der Europäischen Union stetig erhöht. Die europäischen Datenschutzbehörden haben Bußgelder für verschiedene Arten von DS-GVO-Verstößen gegen Unternehmen und Institutionen aus den unterschiedlichsten Sektoren verhängt, etwa aus dem Telekommunikations- und Medienbereich, dem Gesundheitswesen oder dem Finanz- und Versicherungswesen. Häufigkeit und Höhe dieser Bußgelder haben sich seitdem jährlich gesteigert und es ist abzusehen, dass die Behörden ihre Aktivitäten in diesem Bereich weiter ausbauen werden. Dieser Artikel beleuchtet die im Rahmen des Art. 32 DS-GVO von den europäischen Datenschutzbehörden verhängten Bußgelder. Art. 32 befasst sich mit der Sicherheit von Datenverarbeitung und verlangt von der datenschutzrechtlich verantwortlichen Stelle, geeignete technische und organisatorische Maßnahmen zu ergreifen, um sich vor internen und externen Datenschutzverletzungen, Cybersicherheitsverstößen und anderen Vorfällen im Rahmen der Datensicherheit zu schützen. Bis Ende Juni 2021 machten die Bußgelder, die für Verstöße gegen Art. 32 verhängt wurden, ein Fünftel aller bebußten DS-GVO-Verstöße aus.

Schlüsselwörter Cybersicherheit · Interne Datenschutzverletzung · Externe Datenschutzverletzung · Technische und organisatorische Maßnahmen · Art. 32 DS-GVO

1 Methodology

The figures and findings in this article are based on the General Data Protection Regulation (GDPR) fines that have been imposed up until June 2021 following the entry into effect of the GDPR, where the main cause for the fine was a breach of article 32. As not all fines are made public, the dataset of article 32 fines used in this article is not exhaustive: it is a compilation of enforcement decisions that were officially published or confirmed by the national data protection authorities (DPAs).[1] The dataset offers insights into the DPAs' focus areas and on emerging trends. The graphics in this article are based on that dataset and aim to help visualise the findings. Also included are some general insights on GDPR enforcement as a whole, and the impact that the findings of this article might have on organisations is discussed.

[1] The dataset comprises 117 fines that complied with these requirements, which is roughly 1/5 of all 600 publicly available fine decisions by European DPAs as of 22 June 2021.

2 What are organisations being fined for?

Organisations can breach article 32 in various ways; the type of breach determines the severity of the fine and other compliance actions that they may face.[2] To analyse what types of breaches have attracted fines, the authors classified them as: internal or external data breaches; cyber security breaches; and/or technical and organisational measures (*TOM*) *only*. *TOM only* cases are those where an organisation is fined for general non-compliance with article 32 (i.e. has inadequate TOM in place) but no data or cyber security breach has occurred.

A *data breach* is defined in the GDPR as any breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed (article 4.12 GDPR).

The article distinguishes between fines levied for external and internal data breaches. In this article, *internal data breaches* are classified as breaches where either a generally authorised person has destroyed, lost, altered, disclosed or accessed personal data by exceeding his/her authorisation, or where an unauthorised person from within the organisation has performed any of these actions. *External data breaches* are breaches where personal data is manipulated, as defined in article 4.12 GPDR, by any unauthorised person outside the organisation.

The term *cyber security breach* is not defined in the GDPR. Therefore, the definition of cyber security breach is based on the current European Union (EU) network and information systems (NIS) Directive and the EU Cybersecurity Act. The NIS Directive defines cyber security breaches as 'events having an actual adverse effect on the security of network and information systems',[3] i.e. where IT applications, services, networks or devices are accessed (i.e. breached) by bypassing the underlying security mechanism.[4]

3 External data breaches

The dataset shows that, since 2018, 42% (49 out of 117) of the fines for article 32 breaches have been imposed on organisations that DPAs have determined as having suffered from an external data breach. For example, the Danish DPA has issued three fines for article 32 breaches. According to the Danish DPA, all three organisations had suffered from an external data breach.[5] (Similarly, many of the Romanian

[2] See Piltz [2] in Gola DS-GVO (2nd Ed. Art. 32 rec. 54).

[3] Art. 4 para. 7 NIS Directive (EU) 2016/1148.

[4] See Art. 2 para. 1 Cybersecurity Act (EU) 2019/881.

[5] Danish DPA (9 Dec 2020). Press release. Available via https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/dec/kommune-indstillet-til-boede. Accessed 12 September 2021. Danish DPA (4 Aug 2020). Press release. Available via https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/aug/datatilsynet-indstiller-privatbo-til-boede. Accessed 12 September 2021. Danish DPA (30 June 2020). Press release: available via https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/jun/lejre-kommune-indstilles-til-boede. (Accessed 12 September 2021. As explained above, an external data breach is a breach of security by an unauthorised external person that leads to the manipulation of personal data.).

penalties have been issued for external data breaches; these were across a variety of sectors, including financial, technology, media and telecom [TMT] and consumer). The UK Information Commissioner's Office (ICO) has also issued all three of its article 32 fines against organisations that it deemed to have suffered from external data breaches. As of June 2021, two of the three ICO fines[6] were the highest ever GDPR fines. Notably, both fines were reduced because the organisations co-operated with the ICO during its investigation. The Italian DPA has issued the third highest fine, of €27.8 m, against a telecoms company for what it considered to be an external data breach.[7] While some EU DPAs show a particular interest in external data breaches, others have focused less on this type of breach. For example, none of the article 32 fines issued by the Swedish DPA were for external data breaches.

4 Internal data breaches

Roughly 25% (29 of 117) of all fines imposed for article 32 breaches were for internal data breaches.[8] Of the fines imposed for internal data breaches, about 50% were given to organisations that deal with sensitive personal data (e.g. personal health data or children's data).[9] For example, the Dutch DPA has fined two hospitals for internal data breaches where unauthorised staff had access to personal health data.[10] The Portuguese DPA has only issued one penalty for an article 32 breach, which was also to a hospital for what the DPA deemed to be an internal unauthorised manipulation of personal health data.[11] Various German DPAs have also levied fines on organisations for internal data breaches. For example, the DPA of Baden-Wuerttemberg has issued a fine against a financial company for wrongly deleting personal data.[12] Another German DPA, the DPA of Rhineland Palatinate, has fined

[6] Marriott for £18.4 m and BA for £20 m, see ICO's decisions. Available via https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf and via https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf. Both accessed 12 September 2021.

[7] Italian DPA fined TIM SpA, see DPA's decision (15 Jan 2020). Available via https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9256486. Accessed 12 September 2021.

[8] As explained above, an internal data breach occurs when data is unlawfully manipulated by someone within an organisation who was unauthorised to do so or exceeded their authorisation.

[9] Art. 9 GDPR sets out stricter requirements for processing sensitive personal data.

[10] Dutch DPA fined Haga Hospital, see DPA's decision (16 Juli 2019). Available via https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers. Accessed 12 September 2021. The fine was reduced from €460,000 to €310,000. See https://globaldatareview.com/cybersecurity/first-dutch-gdpr-fine-reduced. Accessed 12 September 2021. Amsterdam hospital OLVG, see DPA's decision (11 Feb 2021). Available via https://autoriteitpersoonsgegevens.nl/en/news/olvg-hospital-fined-inadequate-protection-medical-records. Accessed 12 September 2021.

[11] Public Hospital (17 July 2019), see DPA's website. Available via https://www.cnpd.pt/. Accessed 12 September 2021.

[12] DPA Baden-Wuerttemberg (30 July 2019). Press release. P. 2. Available via https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/07/PM-Datenschutzverletzungen-bereiten-zunehmend-Sorge-30.07.2019.pdf. Accessed 12 September 2021.

a hospital[13] for unauthorised staff having access to personal health data, which led to hospital bills being sent to the wrong patients. The Swedish DPA has also shown a particular interest in internal data breaches: six of its 11 penalties for article 32 breaches were for internal data breaches concerning sensitive medical or financial data, with four of those fines being over €1 m.[14]

This suggests that regulators are taking internal data breaches very seriously, especially where sensitive personal data is involved.

5 Cybersecurity breaches

This study also looks at article 32 fine decisions that have been handed down for cybersecurity breaches, within the meaning of the NIS Directive. As the EU DPAs do not have powers to enforce the NIS Directive per se, publicly available information about the facts of the cases was used to determine whether a cybersecurity element was present. Notably, not every article 32 fine includes a cybersecurity element. In fact, only about a fifth of data breaches occurred because the underlying security mechanism was bypassed through IT applications, services, networks or devices.

Interestingly, all cases that included a cybersecurity breach also fell under the definition of an external data breach. This means that the breach of security, which occurred by accessing or bypassing the security of network or information systems, was orchestrated by an unauthorised external person in all cases. Although enforcement against cybersecurity breaches are rarer, the penalties for them are high. For example, the Spanish DPA fined an organisation €600,000[15] for a cybersecurity attack, as it found that the organisation did not have sufficient TOM in place. Similarly, the French DPA fined an organisation €180,000[16] for a cybersecurity breach. In this case, personal accounts were accessible via hyperlinks on search engines, which resulted in many of the accounts being compromised. The French DPA deemed that this gap in the organisation's security system led to the cybersecurity breach and was an infringement of article 32 GDPR.

Given the continuous increase in digital data management, working from home and moves to the cloud, the number of combined data and cyber breaches is likely

[13] DPA Rhineland Palatinate (3 Dec 2019). Press release. Available via https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/geldbusse-gegen-krankenhaus-aufgrund-von-datenschutz-defiziten-beim-patientenmanagement/. Accessed 12 September 2021.

[14] Swedish DPA fined Capio St. Göran's Hospital, see DPA's decision (2 Dec 2020). Available via https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-capio-st-gorans-sjukhus-di-2019-3846.pdf. Accessed 12 September 2021. Aleris Sjukvård AB, see DPA's decision (2 Dec 2020). Available via https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-aleris-narsjukvard-di-2019-3842.pdf. Accessed 12 September 2021. Aleris Sjukvård AB, see DPA's decision (2 Dec 2020). Available via https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-aleris-sjukvard-di-2019-3844.pdf Accessed 12 September 2021. MedHelp, see DPA's decision (7 June 2021). Available via https://www.imy.se/globalassets/dokument/beslut/2021/2021-06-07-beslut-medhelp.pdf. Accessed 12 September 2021.

[15] Air Europa, see DPA's decision (2020). Available via https://www.aepd.es/es/documento/ps-00179-2020.pdf. Accessed 12 September 2021.

[16] Active Assurances, see DPA's decision (18 July 2019). Available via https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038810992/. Accessed 12 September 2021.

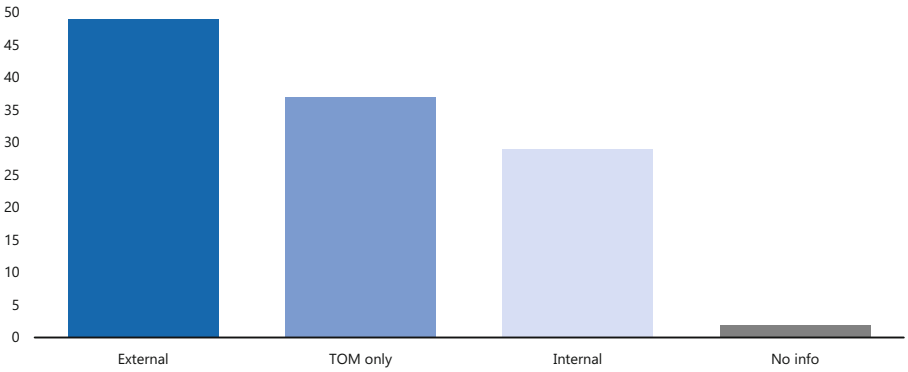

Fig. 1 Types of article 32 General Data Protection Regulation non-compliance. *TOM* technical and organisational measures. (Source: Freshfields research, data correct on 22 June 2021)

to increase. Organisations should be on alert and make sure their security networks are airtight.

6 Technical and organisational measures

In all cases where article 32 fines were issued for data or cyber breaches, EU DPAs found that there had been insufficient TOM. In all, 31% (36 of 117) of the fines were for insufficient TOM alone (i.e. there was no data or cyber breach). When a data or cyber breach occurs, DPAs tend to see this as a sign that the TOM were insufficient: appropriate TOM should, by definition, prevent breaches from happening. DPAs will also assess the scope of TOM in place when setting any fines. This means that having effective TOM in place can be beneficial for organisations even if a data or cyber breach occurs.[17] Organisations should regularly revisit their TOM to keep them up to date.

Figure 1 shows how many fines were given for each of the different types of article 32 GDPR since the GDPR became effective up until June 2021. It distinguishes between internal or external data breaches and TOM only cases, i.e. where DPAs found that inadequate TOM were in place but where no data breach had occurred.

7 National trends

Significant national trends in relation to article 32 breaches were identified. For example, some regulators focus on data breach and data security incidents in general, while others target specific sectors or types of breach.

Figure 2 shows how many fines the DPAs in each European country have issued for article 32 GDPR infringements.

[17] Piltz [2] in Gola DS-GVO (2nd Ed. Art. 32 rec. 54–56).

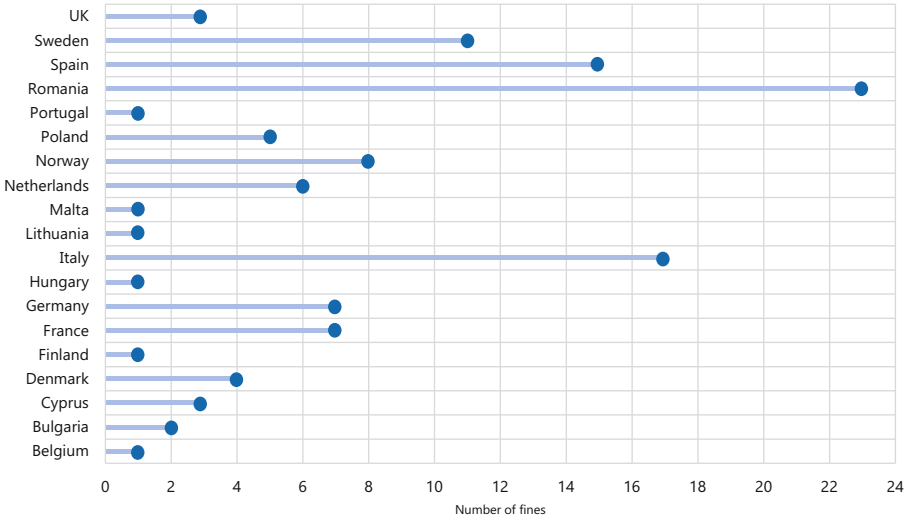

Fig. 2 Article 32 General Data Protection Regulation enforcement activities by country. (Source: Freshfields research, data correct on 22 June 2021)

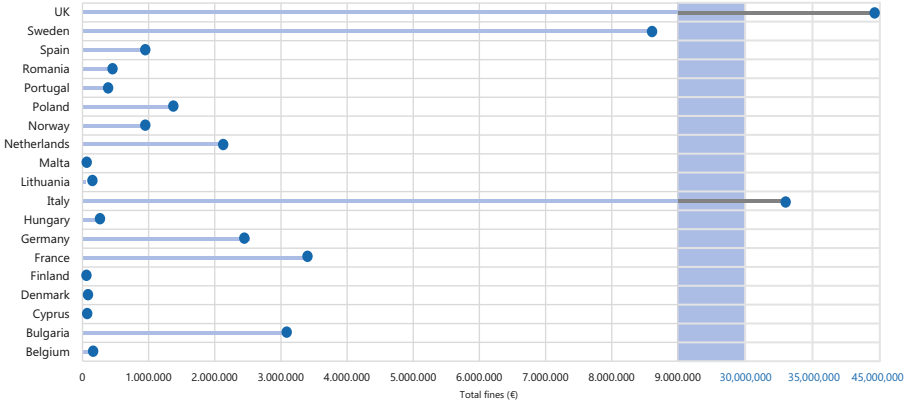

Fig. 3 Total value of fines for article 32 General Data Protection Regulation non-compliance by country. (Source: Freshfields research, data correct on 22 June 2021)

Figure 3 shows the total value of fines the DPAs in each European country have issued for article 32 GDPR breaches.

UK The ICO issued four GDPR fines between 2018 and June 2021.[18] Three of those four cases involved an article 32 breach—specifically an external data breach.

[18] See ICO's decisions: Marriott (30 Oct 2020). Available via https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf. British Airways (16 Oct 2020). Available via https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf. Doorstep Dispensary (17 Dec 2019). Available via https://ico.org.uk/media/action-weve-taken/enforcement-notices/2616741/doorstop-en-20191217.pdf. Ticketmaster (13 Nov 2020). Available via https://ico.org.uk/media/action-weve-taken/2618609/ticketmaster-uk-limited-mpn.pdf. All accessed 12 September 2021.

This suggests that the ICO's focus is on external data breaches. The combined total of the three fines is €44.4 m, which means that the average fine is €14.8 m. These penalties are some of the highest fines that have been issued under the GDPR as of June 2021. The ICO has repeatedly noted that co-operating with the regulator can significantly lower the penalty and encourages organisations to do so.

Italy The Italian DPA (Garante) is currently one of Europe's more active regulators.[19] This also holds true when it comes to data breaches and data security incidents. Within the last 3 years, the Garante has issued 17 fines for article 32 breaches.[20] Many of these fines were given to universities and local municipalities, suggesting that the Garante is coming down hard on public and governmental institutions. The highest fine issued by the Garante is for €27.8 m.[21] The Garante noted that the organisation had repeatedly failed to correct the shortcomings that it had pointed out.

Romania The Romanian DPA also shows a particular interest in data breaches and data security incidents. As of June 2021, it had issued the most article 32 fines (23) of all the EU DPAs.[22] Although the fines are at the lower end of the spectrum (ranging from €500 to €10,000), the DPA targets organisations across a variety of sectors, including financial, TMT and consumer.

Spain The Agencia Española de Protección de Datos (AEPD) is generally known as Europe's most active data protection regulator. It has issued over 200 penalties since the GDPR came into force.[23] The AEPD does not seem to particularly focus on data breaches and data security incidents but imposed about 15 fines for them.

Sweden The Swedish DPA has issued 11 penalties for data breaches or data security incidents, totalling €8.62 m; this averages out to €784,000. The regulator has repeatedly targeted organisations in the healthcare sector and public institutions that process sensitive personal data, such as health data or children's data.

France The French DPA (Commission Nationale de l'Informatique et des Libertés, CNIL) has issued seven penalties for article 32 breaches. It levied a single fine of €2.25 m on an organisation[24] that it deemed had insufficient TOM in place. Notably,

[19] See European Data Protection Board (2021). Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities. Available via https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v2_0.pdf. Accessed 12 September 2021.

[20] See Italian DPA's website. Available via https://www.garanteprivacy.it. Accessed 12 September 2021.

[21] TIM S.p.A., see above.

[22] See Romanian DPA's website. Available via https://www.dataprotection.ro/index.jsp?page=Informatii_plata_amenda_persoane_juridice_2016. Accessed 12 September 2021.

[23] See Spanish DPA's website. Available via https://www.aepd.es/es. Accessed 12 September 2021.

[24] Carrefour France, see French DPA's decision (18 Nov 2020). Available via https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042563756. Accessed 12 September 2021.

two of the seven penalties were for breaches that included a cybersecurity element.[25] The two penalties related to the same incident, but the CNIL decided to fine the data controller and the data processor individually—this is rare, but is possible.[26]

Germany Generally, most of the German DPAs do not seem to focus particularly on article 32 breaches, instead spreading their enforcement activities across a variety of GDPR breaches.[27] However, the DPA of Baden-Wuerttemberg seems to be Germany's primary watchdog when it comes to article 32. Of the seven article 32 fines issued by German DPAs,[28] five were levied by the DPA of Baden-Wuerttemberg. The highest penalty it has issued is for €1.24 m, for insufficient TOM and unlawful data processing in the context of direct marketing.[29] The seven German fines amount to €2.52 m in total.

Netherlands The Dutch DPA (Autoriteit Persoonsgegevens, AP) has imposed six fines[30] for article 32 breaches, with most being in the six-digit range; this is at the higher end of the EU spectrum. When looking at fines given for data breaches and data security breaches, the AP seems to focus on the healthcare sector and on infringements involving sensitive personal data. For example, it separately fined two hospitals for internal data breaches involving sensitive personal data where it held that unauthorised staff had access to personal health data.[31]

[25] See French DPA's press release (27 Jan 2021). Available via https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant. Accessed 12 September 2021.

[26] See Art. 58, 83 para. 3 GDPR. See also Klug [3] in Gola DS-GVO (2nd Ed. Art. 28 rec. 18–20). Another example where a controller and a processor were fined for the same case is the Swedish fine decision against AP Voive and MedHelp.

[27] Freshfields (2021) Global Data Risk [1].

[28] AOK, see press release DPA Baden-Wuerttemberg (30 June 2020). Available via https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-bussgeld-gegen-aok-baden-wuerttemberg-wirksamer-datenschutz-erfordert-regelmaessige-kontrolle-und-anpassung/. Accessed 12 September 2021. Hospital, DPA Rhineland Palatinate (3 Dec 2019), see above. Financial company and digital publication, see for both DPA Baden-Wuerttemberg (30 July 2019), see above. Knuddels, see press release DPA Baden-Wuerttemberg (22 Nov 2018). Available via https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/. Accessed 12 September 2021. 1&1 Telecom, see decision from Regional Court Bonn (11 Nov 2020) reducing the fine issued by Federal DPA. Available via https://www.dsgvo-portal.de/assets/img/articles/Pressemitteilung_LG_Bonn_1und1_OWi_1-20_LG_Seite_1.jpg. Accessed 12 September 2021. Grocery store, see DPA Baden-Wuerttemberg (2019) Tätigkeitsbericht. Available via https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/01/35.-T%C3%A4tigkeitsbericht-f%C3%BCr-den-Datenschutz-Web.pdf#page=44&zoom=100,0,0. Accessed 12 September 2021.

[29] AOK, see above.

[30] Haga Hospital and Amsterdam Hospital, see DPA's decisions (16 July 2019) (11 Feb 2021) see above. UWV, see DPA's decision (31 May 2021). Available via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_uwv_beveiliging_groepsberichten.pdf. CP&A, see DPA's decision (24 March 2020). Available via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_cpa_verzuimregistratie.pdf. Orthodontic Clinic, see DPA's decision (4 Feb 2021). Available via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_orthodontiepraktijk.pdf. UWV, see DPA's press release (30 Oct 2018). Available via https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-dwingt-uwv-met-sanctie-gegevens-beter-te-beveiligen. All accessed 12 September 2021.

[31] See above.

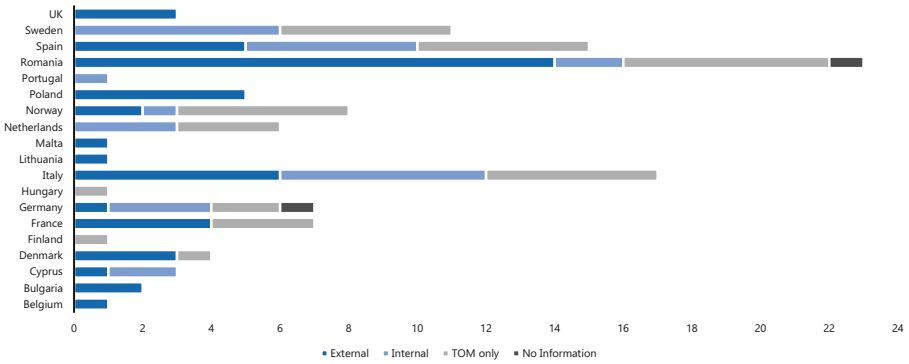

Fig. 4 Types of article 32 General Data Protection Regulation non-compliance by country. *TOM* technical and organisational measures. (Source: Freshfields research, data correct on 22 June 2021)

Figure 4 shows how many fines were imposed for each of the different types of article 32 GDPR infringements by country. It distinguishes between internal or external data breaches and TOM only cases, i.e. where DPAs found that inadequate TOM were in place but where no data breach has occurred.

8 Conclusion: what does this mean for organisations?

The key takeaway from this article is that the EU DPAs are coming down hard on article 32 breaches. Every organisation can, and most likely will, suffer a data and/or cyber breach at some point. They should focus on making sure that they have sufficient TOM in place, as DPAs can and will issue fines for insufficient TOM alone. Organisations should regularly update their TOM: this will help to minimise the risk of a breach and might also reduce any fine if there is a breach.[32] The fines for article 32 breaches can, as explained above, be very high—and it can be predicted that enforcement action will only continue to increase.

References

1. Freshfields Report (2021) Global Data Risk. https://www.freshfields.com/49661d/globalassets/our-thinking/campaigns/digital/cyber-attacks-data-breaches-and-litigation/global-data-enforcement/gpr-report.pdf. Accessed 15 Sept 2021
2. Piltz C (2018) Art. 32 DS-GVO. In: Gola (ed) Datenschutzgrundverordnung, 2nd edn. Beck, München
3. Klug C (2018) Art. 28 DS-GVO. In: Gola (ed) Datenschutzgrundverordnung, 2nd edn. Beck, München

Julia Utzerath LL.M. (Exeter), Maître en droit (Nantes), Rechtsanwältin, Senior Knowledge Lawyer IP/IT/Data

Rhea Dennis Knowledge Executive IP/IT/Data

[32] See Piltz [2] in Gola DS-GVO (2nd Edition Art. 32 rec. 20).