GDPR Today

Edition No. 3
March 2019

European Commission urged to investigate Romanian GDPR implementation

GDPR loopholes facilitate data exploitation by political parties

Uber drivers demand their data

After Brexit, the EU must decide if UK data protection is adequate

OPEN RIGHTS GROUP

EDRi

OPEN SOCIETY FOUNDATIONS

Editorial

Welcome to GDPR Today – your online hub for staying tuned to the (real) life of EU data protection law. As you know, every two months we publish statistics showing how the GDPR is being applied across Europe. We also share relevant news, from legal guidelines and decisions to data breaches, new codes of conduct, important business developments, and – of course – memes.

This edition brings you data from ten national data protection authorities on the implementation of the GDPR. Although this is a smaller number than we would have liked, it is encouraging to be able to report that nearly one year on since the GDPR came into force, complaints and data breaches continue to be notified with regularity. Check out our "GDPR in Numbers" section to see how the law is being used in practice.

The last couple of months have seen a flurry of GDPR activity, at both national and EU institutional level. Authorities in Germany, the Netherlands and Spain have issued strong statements, interpretations and rulings challenging how personal data is used by online platforms and political parties and calling for increased privacy protections. The European Data Protection Board and Supervisor have both issued reports which showcase how GDPR is being applied at EU level. Only just this week, European Commissioner Věra Jourová made a forthright conference speech extolling the benefits that the GDPR is bringing to businesses and citizens, both within the EU and globally.

Not all is positive progress. It is disappointing that the European Commission has still not yet taken action to ensure that Romania properly implements the GDPR. There are also several countries which have yet to publish any GDPR data. These gaps in transparency and enforcement dangerously undermine the consistent application of the GDPR across all EU Member States.

We all have a role to play in making data protection a reality. Here at GDPR Today, we will continue monitoring and reporting on these efforts, and we look forward to seeing continuing improvement by businesses, States and international institutions.

Amy Shepherd, Open Rights Group

The content and data presented in this edition was provided by:

Access Now

Association for Technology and Internet

Bits of Freedom

Data Skydd

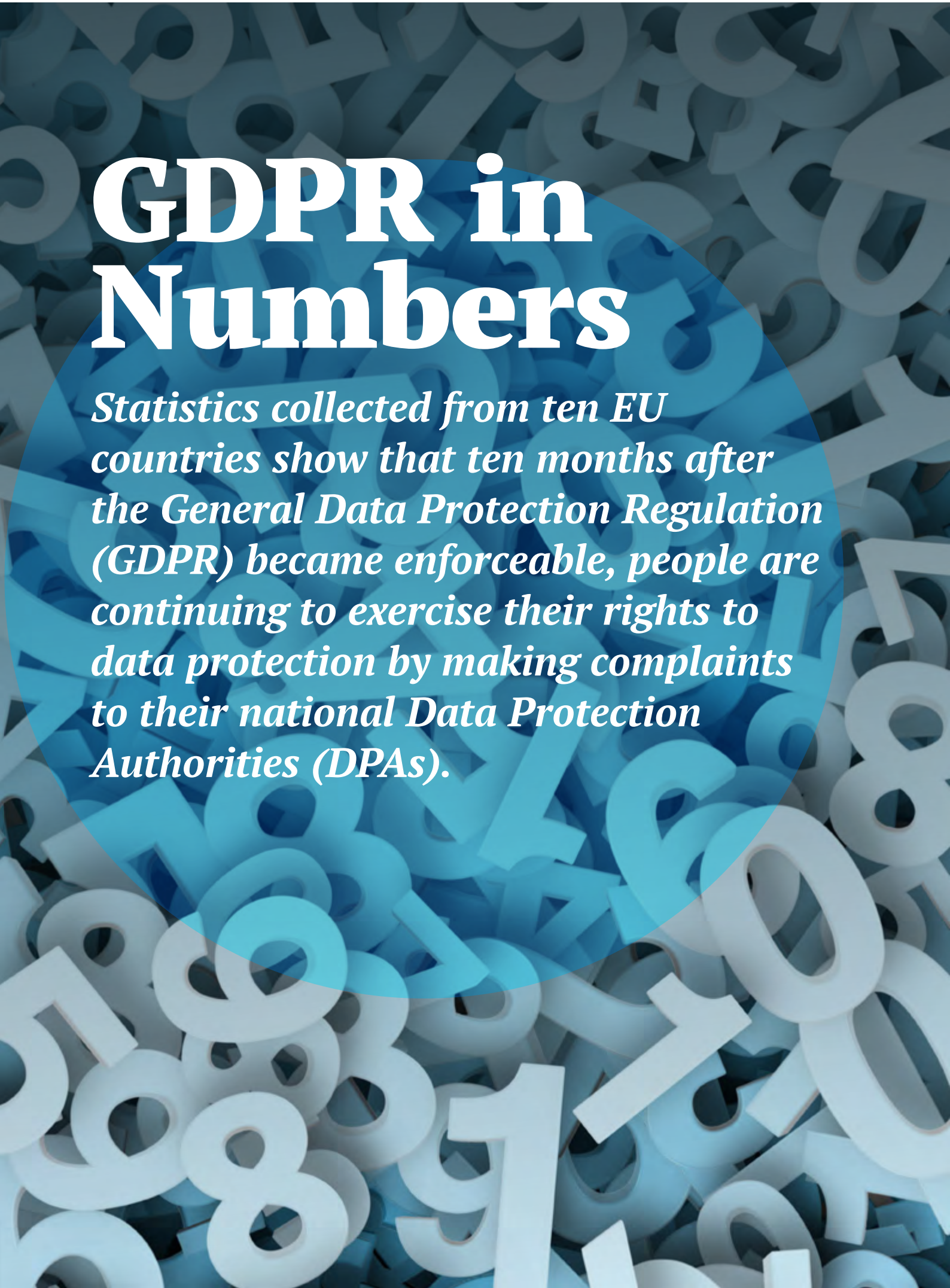
Homo Digitalis

Open Rights Group

NOYB

Panoptykon Foundation

Privacy International



GDPR in Numbers

Statistics collected from ten EU countries show that ten months after the General Data Protection Regulation (GDPR) became enforceable, people are continuing to exercise their rights to data protection by making complaints to their national Data Protection Authorities (DPAs).

Almost a year into GDPR implementation, people across the EU are continuing to exercise their data protection rights and raise issues with national enforcement authorities.

COUNTRIES COVERED IN THIS EDITION

For this edition, we were able to obtain comprehensive data on DPA activity from ten EU Member States. This was fewer than the last edition. Some countries indicated that they were unable to supply data in the request time-frame due to preparation of annual reports. We are disappointed not to have a wider dataset for this edition but expect to be able to obtain data on more countries in future issues.

The charts below present statistical data provided by the DPAs from Austria, Cyprus, Germany, Greece, Ireland, Italy, Poland, Sweden and the United Kingdom. We did not have data for Austria, the United Kingdom, Ireland or Hungary in the previous issue.

The reference dates covered for each of the countries differs slightly (see details below for individual countries), but overall this data covers 25 May 2018 to 1 March 2019.

We are presenting statistics about:

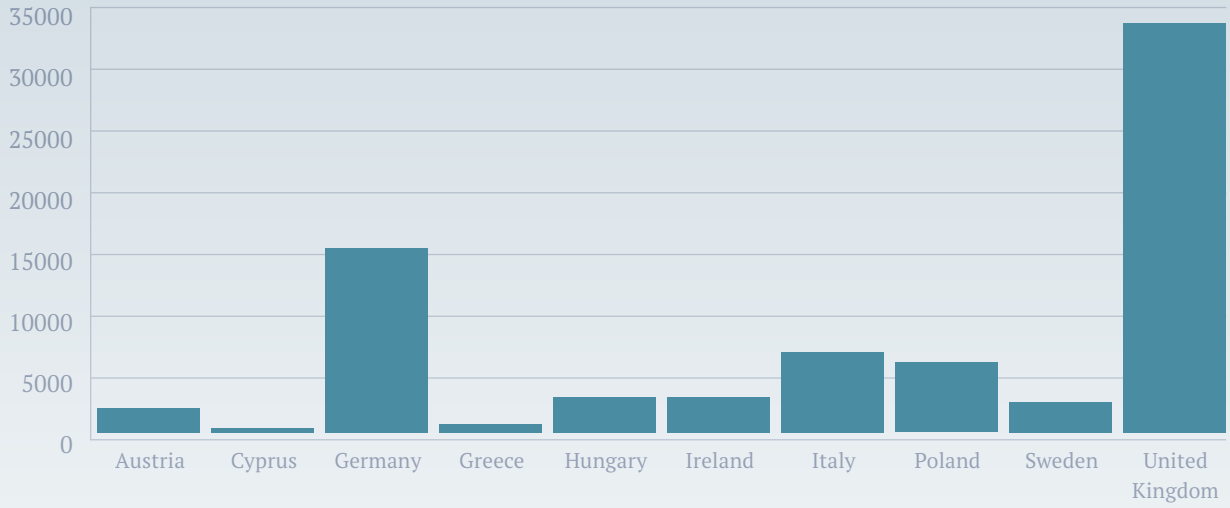
- ***the total number of complaints received, and***
- ***the total number of data breach notifications received.***

Getting the data – what are the challenges?

Collecting comparable data across the EU for this publication is a resource-intensive process, which we currently struggle to accomplish due to insufficient resources. It is made additionally complex by the lack of consistency in how national DPAs record, store and supply GDPR data. Some countries such as Ireland simply refer us to officially published reporting. In other cases, it is possible to request data directly from national DPAs. Even then, DPA responses vary, which makes comparative analysis difficult.

Germany presents a particular challenge for data collection, since it has a separate data protection authority for each of its 16 federal states. This means we would need to obtain data from each federal DPA to accurately report on GDPR compliance across the country as a whole. However, some federal states, including the highly populated state of Bavaria, have yet to provide any data about the number of complaint or data breach notifications they have received since the GDPR came into effect in 2018. This means any reporting on Germany is likely to be undercounting, potentially significantly, the true number of complaints and data breach notifications across the general population.

We again ask the European Data Protection Board (EDPB) to develop protocols which require and explain how national DPAs should publicly report specifically comparable figures at frequent and regular intervals. Ad hoc and annual reporting is not precise enough to properly analyse the impact of GDPR.



Complaints

The number of complaints submitted to the DPAs. Lawsuits filed with courts are not included.

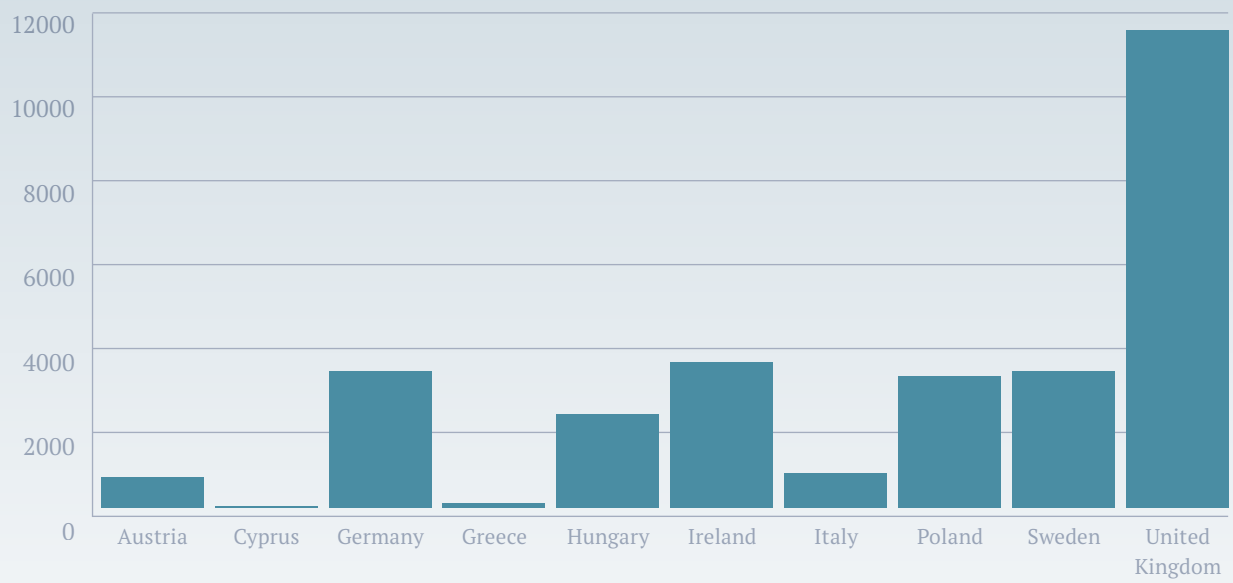
The numbers show that a significant number of complaints have been filed across the EU. Every country where we have previous data has had new complaints in this reporting cycle.

Putting the number in context

The data shows that the United Kingdom's DPA is receiving vastly more complaints than other countries in terms of raw numbers. However, looking at this against the number of individuals in the country (per capita), the UK has had roughly 51 complaints per 100,000 people. Looking at this against other per capita data presents a different picture of the UK DPAs activity.

Ireland has had relatively few complaints overall, but has had roughly 57 complaints per 100,000 people. This is higher than the UK. The reporting period for Ireland was around two months shorter than the other countries in this report, however, so there is some undercounting here. Hungary has had an average of approximately 10 complaints per day in this reporting period and around 29 complaints per 100,000 people. This is higher than Poland, for example, which had more complaints overall but on a per capita basis had around 15 complaints per 100,000 people.

Collecting comparable data across the EU for this publication is a resource-intensive process, which we currently struggle to accomplish due to insufficient resources.



Breach Notifications

The number of data breach notifications submitted to Data Protection Authorities by businesses or other organisations, pursuant to Article 33 of the GDPR.

As with complaints, the UK DPA received the most breach notifications – an average of around 42 per day over the course of the reported period. Ireland had many fewer notifications in terms of raw numbers, but had around 70 notifications per 100,000 people over their reporting period. This is possibly due to the large number of businesses which have their headquarters in Ireland. Sweden is also receiving a relatively large number of breach notifications – 33 per 100,000 people.

The absence of the Netherlands in this dataset skews the UK's position as against other countries, since in the last reporting cycle, the Netherlands had 12,763 breach notifications, over 1000 more than the UK.

What's next?

The conclusions above are based on a very small data sample. However, they are supported by other published reporting. The EDPB gave a figure of over 95,000 complaints in its first overview report[1] on the implementation of the GDPR. Law firm DLA Piper also reported a total of over 59,000 data breaches in this February 2019 survey[2]. Taken together, these figures indicate that even in this "transition year" (a term used by French regulation Mathias Moulin at a recent conference[3]) the notification element in the GDPR is working well.

Public data is important. Transparency helps to increase consistency, and other countries, particularly the United States, are watching[4] to see how GDPR performs and where its strengths and weaknesses lie. As GDPR reaches its first birthday in May, DPAs across the EU will be preparing annual reports, which should give us a wider picture of compliance. We're particularly interested in seeing how Slovakia, Bulgaria, Croatia, Estonia and Lithuania are performing, as data on these countries is currently scarce.

DETAILS CONCERNING DATA COLLECTION IN INDIVIDUAL COUNTRIES

GDPR Today will be collecting statistical information from DPAs in bi-monthly rounds – Stay up to date!

Austria
25 May 2018 to 1 March 2019; figures gathered by NOYB[5]

Cyprus
25 May 2018 to 1 March 2019; figures gathered by Homo Digitalis[6]

Germany
The period covered varies by federal state. For most states, the time frame is 25 May 2018 to around 1 March 2019; figures gathered by Panoptykon Foundation[7]

Greece
25 May 2018 to 1 March 2019; figures gathered by Homo Digitalis[8]

Hungary
25 May 2018 to 1 March 2019; figures gathered by Access Now[9]

Italy
25 May 2018 to 1 March 2019; figures gathered by NOYB[10]

Ireland
25 May – 31 December 2018; figures gathered from Ireland's Data Protection Commission Annual Report for 2018[11]

Poland
25 May 2018 – 28 February 2019; figures gathered by Panoptykon Foundation[12]

Sweden
25 May 2018 to 18 March 2019; figures gathered by Data Skydd[13]

United Kingdom
25 May 2018 to 31 January 2019; figures gathered by Open Rights Group[14]

[1] http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf

[2] https://www.dlapiper.com/en/uk/news/2019/02/dla-piper-gdpr-data-breach-survey/

[3] https://www.theregister.co.uk/2019/03/14/more_than_200000_gdpr_cases_in_the_first_year_55m_in_fines/

[4] https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html

[5] https://noyb.eu

[6] https://www.homodigitalis.gr

[7] https://panoptykon.org

[8] https://www.homodigitalis.gr

[9] https://www.accessnow.org

[10] https://noyb.eu

[11] https://www.dataprotection.ie/sites/default/files/uploads/2019-02/DPC%20Annual%20Report%2025%20May%20-%2031%20December%202018.pdf

[12] https://panoptykon.org

[13] https://dataskydd.net

[14] https://www.openrightsgroup.org

European Commission urged to investigate Romanian GDPR implementation

ISSUE

The Romanian law implementing the General Data Protection Regulation (GDPR) allows national political parties to process personal data, including sensitive data, in a manner that disregards citizen rights. Law no. 190/2018[1] excludes the need to acquire consent for processing personal data, including sensitive data. This effectively gives political parties a "carte blanche" to process political opinions and personal data unrestrictedly, with no real safeguards in place.

Civil society organisations across the EU have long warned that the "flexibilities"[2] in GDPR allowing for diverging national implementation measures will lead to differences in the level of protection applicable in Member States. In Romania, the derogations allowed by Law no. 190/2018 are seriously weakening the protections and safeguards the Regulation envisions. They allow the State to disregard basic data protection principles and breach EU law. Paradoxically, they even lower the level of data protection provided by the previous national law which implemented the Data Protection Directive 95/46/EC which preceded the GDPR.

COMPLAINT

On 14 February 2019, the Association for Technology and Internet (ApTI) sent a complaint[3] to the European Commission which outlined the following problems with Romania's GDPR implementation law:

1. ***Political parties and organisations are allowed to process personal data, including sensitive data without consent and appropriate safeguards, thus disregarding data protection principles.***

The derogations prescribed under Romanian law allow political parties, citizen organisations belonging to national minorities and not-for-profit organisations to process special categories of personal data without explicit consent or appropriate safeguards.

The only processing requirements are (1) to inform the data subject that personal data processing is taking place, and (2) to show the mechanisms through which the data subjects can exercise their rights to rectification and deletion (which is mandatory anyway according to GDPR Articles 13-14).

In creating this consent exception, Romanian law seems to rely on Recital 56 of the GDPR, which states that political parties can compile personal data on people's political opinions for reasons of public interest if the Member State's electoral system requires them to do so. However, this is an explanatory text, not a binding provision, and it does not intend to eliminate the need for political parties and organisations to have and show a legal basis to process personal data. Concerningly, Romanian law no. 190/2018 excludes the need to have consent without indicating which legal basis does apply.

2. Processing of personal data for journalistic purposes is very limited and could block publishing of public interest stories.

There are three situations in the Romanian law under which data can be processed for journalistic purposes: (1) if the processing concerns personal data which was clearly made public by the data subject; (2) if the personal data is tightly connected to the data subject's quality as a public person; (3) if the personal data is tightly connected to the public character of the acts in which the data subject is involved.

If any of these situations applies, the GDPR (save for the chapter on sanctions) is entirely excluded from application.

These derogation scenarios are extremely limited compared with those permitted by the European Court of Justice and the European Court of Human Rights. Concerns[4] have already been raised in relation to investigatory news outlet the RISE Project[5] that the GDPR could be used as a tool to silence freedom of the press. The actions of the Romanian Data Protection Authority (DPA) in connection to RISE Project publication by seeking disclosure of the source of personal data that might reveal the journalists' sources and also "access" to that data represent a clear threat to freedom of expression and information.

3. Derogations for public authorities lead to avoid in application of the GDPR in the public sector.

Under Romanian law 190/2019, the DPA must issue tailor-made "remedy plans" for public authorities engaged in data protection violations. In cases of non-compliance with these plans, the DPA can issue fines of between 10 000 and 200 000 RON (approximately between 2 104 EUR and 42 091 EUR). This is an incredibly low upper fine limit in comparison across the EU.

The issuing of remedy plans creates a problematic situation: no matter how serious the data violation is, the public authority will take no responsibility but will simply wait for the DPA to present its remedy plan. There is no incentive for the public authority to take active remediation measures or to think independently about how it could practically implement the GDPR. Evidence of this can be seen in practice[6] already. The low fines also encourage the public authorities to continue "business as usual" without awarding more attention to individual protection.

ACTION AND RESPONSE

These issues raise serious concerns about Romania's ability to properly implement and enforce GDPR. ApTI's complaint offers an important opportunity for the European Commission to firmly intervene and make sure that fundamental rights are protected and the application of the GDPR is consistent across all Member States.

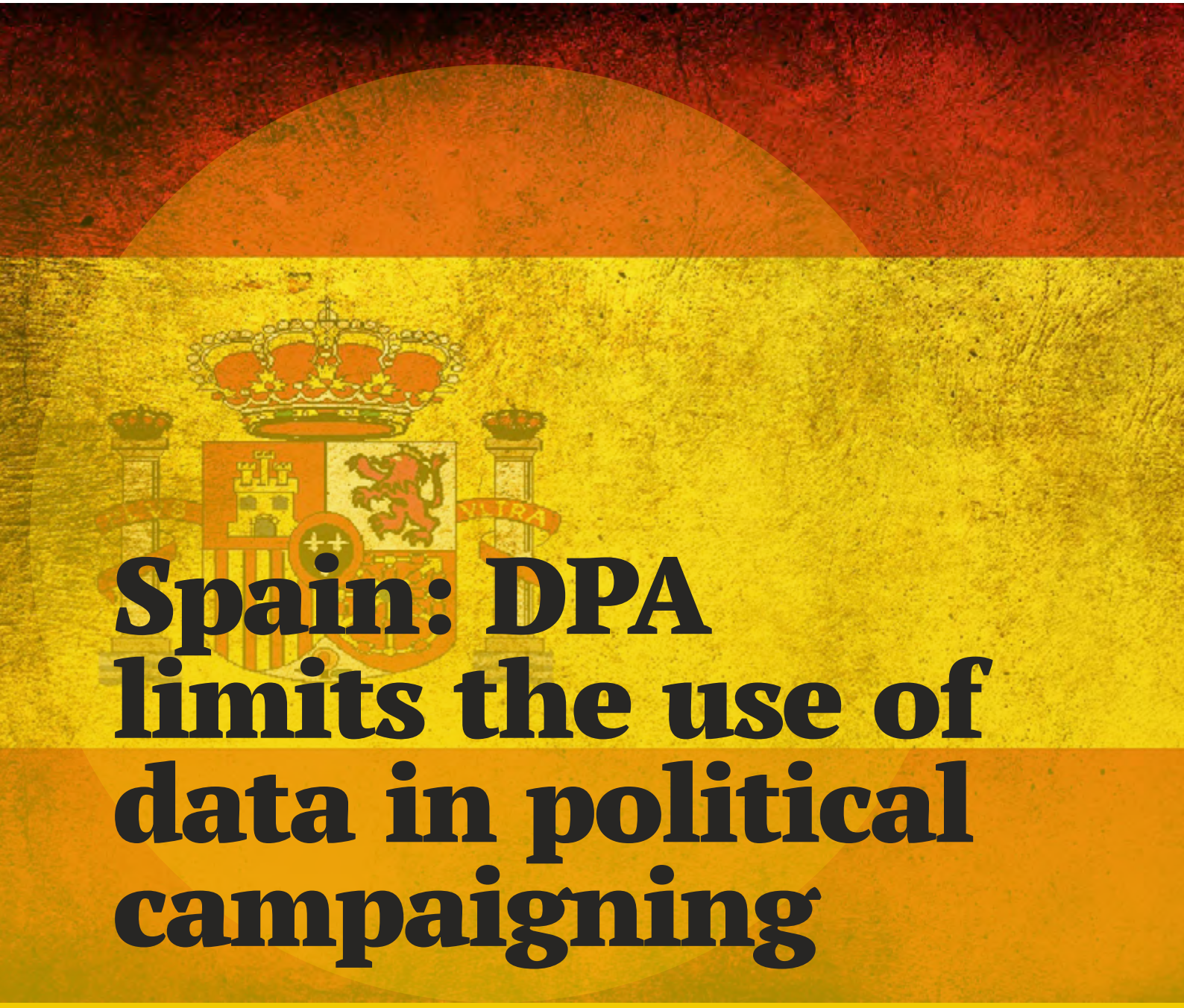
The issues outlined above have been raised by Member of the European Parliament Sophie in't Veld in a letter[7] to the European Commission and in a Parliament hearing[8] on the implementation of the GDPR. However, the European Data Protection Board (EDPB) and the European Commission have both failed to offer concrete action points in terms of redressing the incorrect application of the GDPR and the differences in implementation in different countries.

The problem with GDPR is particularly acute in Romania, but the issues are mirrored across the EU, as other Member States such as Spain and the UK have also used the derogation opportunities to implement GDPR in ways that do not adequately protect personal data.

GDPR is intended as a strong instrument to protect and guarantee rights; not just data protection and privacy but also freedom of expression and other political rights. However, its power is currently being diminished by poor national legislation and policy. We urge the European Commission, the EDPB and all national DPAs to take action to ensure that GDPR national implementing legislation fulfils its intended purpose.

By Valentina Pavel, Mozilla Fellow at Privacy International and Association for Technology and Internet (ApTI) member

[1] https://iapp.org/media/pdf/resource_center/Romanian_Data_Protection_Law_English_Translation.pdf
[2] https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf
[3] https://www.apti.ro/sites/default/files/Complaint%20on%20Romanian%20implementation%20of%20the%20GDPR%20-%20ApTI.pdf
[4] https://www.apti.ro/sites/default/files/ApTI%20and%20PI%20letter%20to%20EDPB%20-%20RISE%20Project.pdf
[5] https://privacyinternational.org/blog/2456/teleormanleaks-explained-privacy-freedom-expression-and-public-interest
[6] https://privacyinternational.org/blog/2456/teleormanleaks-explained-privacy-freedom-expression-and-public-interest
[7] https://twitter.com/SophieintVeld/status/1100683179747405824
[8] http://www.europarl.europa.eu/ep-live/en/committees/video?event=20190226-0900-COMMITTEE-LIBE



Spain: DPA limits the use of data in political campaigning

The Spanish Data Protection Authority (DPA), the Agencia Española de Protección de Datos (AEPD), has issued a notification[1] *(circular)* on the use of political data during elections that could shake the foundation of political campaigning online.

The notification is a legally binding document under Article 55 of the Spanish Data Protection Law of 2018, which implements the General Data Protection Regulation (GDPR). It interprets Article 58 of the Spanish law, which complements GDPR provisions on the use of technology and personal data in election activities. Article 58 has been widely perceived in Spain as being too permissive: societal concerns about data misuse by political parties prevail after several corruption scandals and the Catalan crisis. With a social mandate to clamp down, AEPD's notification sets some of the most restrictive conditions for political campaigning in Europe.

The notification asserts that certain safeguards are needed to permit parties to collect personal data related to political opinions during election periods. It contends that if national legislators failed to include such safeguards in the GDPR implementation law, it is the duty of the AEPD to set these out, without prejudice to measures taken by other authorities, including Spanish electoral regulators.

The notification sets out a list of general GDPR-based safeguards that it insists Spain must implement, such as the need for a Data Protection Officer (DPO), a Data Protection Impact Assessment (DPIA) and security measures for processing high risk data. In addition to this, it goes much further. It states that for personal data to be used in election campaigning it must have been "freely expressed" – not just with free will but in the strictest sense of an exercise of the fundamental rights to free expression and freedom of political opinion protected by Articles 16 and 20 of the Spanish Constitution.

The "freely expressed" provision puts an incredibly tight rein on how political parties can process personal data. According to the notification, they're allowed to obtain political data from the web or other public sources but not from private messaging groups, excluding the possibility to obtain data from services such as WhatsApp or Telegram. They might not be able to use data obtained from data brokers and definitely can't infer political ideology through the use of big data or artificial intelligence techniques.

This extremely restrictive approach is justified by the need to protect fundamental rights enshrined in the Spanish Constitution. It is also predicated on GDPR provisions. Importantly, the Spanish legislator in its Data Protection Law opted to use the exemption allowed by Article 9(2) GDPR to not permit consent as one of the legal bases to enable the processing of special category data, and only allow for processing in the public interest. This created an imperative for the AEPD to be restrictive in relation to political campaigning, which it labels a "high risk" activity due to both scale and sensitivity.

Even more controversially than this, however, the notification goes on to ban any form of data processing that attempts to influence (desviar) the will of voters, claiming that such processing is not proportionate under GDPR requirements. The practical implementation of this measure may prove extremely difficult. The notification explicitly mentions "microtargeting" as a disproportionate activity, without defining what this is – a point that Spanish critics have already picked up in media coverage. A key aspect of political campaigning is also trying to change the mind of undecided voters, so where will the line be drawn?

The AEPD notification is one of the most direct challenges to the power of social media companies from a European Data Protection Authority.

The notification further restricts profiling activities. People can only be classified at the level of general characteristics. Profiling is not permitted at the individual level or on the basis of very specific personal characteristics. This means that political parties are only allowed to generate insights over the behavioural patterns of aggregate groups, not individuals. Clearly, this is the corollary of the microtargeting ban.

When all put together, the AEPD notification is one of the most direct challenges to the power of social media companies from a European Data Protection Authority. The measures in the document would completely stop the kind of political campaigning seen, for example, during the UK's Brexit referendum in 2016. The complication with its enforcement, however, is that most political parties are already engaging in the activities it aims to prohibit. Both Facebook and Google have dedicated sales teams targeting politicians and vying for advertising budgets to be spent on their platforms.

Whilst the notification is a strong statement of intent, it is unclear whether the AEPD will manage to turn the tide on political campaigning alone, or whether a broader European effort will be required. Ultimately, to make any real difference, the collaboration of internet companies will be central. However, it is hard to see how they would go along with something that fundamentally undermines their whole business model.

By Open Rights Group

[1] https://www.boe.es/boe/dias/2019/03/11/pdfs/BOE-A-2019-3423.pdf

Netherlands: DPA rules websites must allow people to refuse tracking cookies

Websites that allow visitors access only if they accept tracking cookies or comparable ways to track and record visitor behaviour do not comply with the General Data Protection Regulation (GDPR). That is the main message of the standard interpretation[1] published by the *Autoriteit Persoonsgegevens*, the Dutch Data Protection Authority (DPA), on 7 March 2019.

The DPA received dozens of complaints from visitors of websites who were denied access after refusing to allow tracking cookies. The DPA announced that it will intensify its compliance checks and has sent a letter of warning to several potential offenders.

In the interpretation, the head of the DPA emphasised the importance of getting meaningful permission to track in order to protect the privacy of visitors of a website. He noted that only when permission is requested in a good manner will people be able to "consciously and correctly" make use of their right to the protection of their personal data. Otherwise, people give up personal information under pressure, and that is unlawful.

Only when permission is requested in a good manner will people be able to "consciously and correctly" make use of their right to the protection of their personal data.

Consent must be free

Visitors of websites should be able to rely on their personal information being well protected. The GDPR prescribes the legal bases on which processing of personal information has to be based, the main one of which is user consent.

Consent is why many websites ask users for permission to use tracking technologies like cookies, tracking pixels or browser fingerprinting. Users do not need to consent to technologies which are needed for functioning of the website or which allow for a general visitor-analysis of the website. Permission is needed where the behaviour of individual visitors is analysed and tracked in a more thorough manner, or if this information is shared with third parties. This permission should be given without any form of pressure.

Cookie walls leave no free choice

In case of so-called "cookie walls" on websites (where if users do not accept to be tracked they will not be granted access), permission is not given in a free manner. Based on the GDPR, permission is not "free" or without pressure when there is no real or free choice. This includes the situation wherein a refusal to give permission has negative consequences, such as being denied access.

Compliance will be enforced

Now that the DPA has published this interpretation, websites will have to adjust their practices. Already, the websites for which the DPA have received the most complaints have received a letter with the interpretation and an announcement of intensified checks by the DPA to see whether the GDPR rules are applied in the correct manner.

There is no permission like free permission

Bits of Freedom welcomes this strict interpretation of the GDPR by the Dutch DPA. There is no permission like free permission, and a permission when access is denied in case of refusal is not free. The legal basis of consent is frequently misused, making the statement of the DPA especially timely. Bits of Freedom considers that free permission should include a truly informed form of consent. Cookie statements that are endlessly long or unnecessarily incomprehensible, and/or which steer people towards saying "yes" without genuinely knowing what they are agreeing to, are not acceptable.

Hopefully, this interpretation will spark the entrepreneurial zeal of website owners. It is time for sites to start investigating and investing in business models that do not require the unnecessary and unlawful processing of personal information.

By Lotte Houwing, Bits of Freedom

[1] https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies

GDPR loopholes facilitate data exploitation by political parties

Elections, referendums and political campaigns around the world are becoming ever more sophisticated data operations[1]. This raises questions about the political use and abuse of personal data. With the European Union elections fast approaching and numerous national and local elections taking place across EU Member States, it is essential that the legal frameworks intended to protect our personal data do just that.

Member State laws that implement General Data Protection Regulation (GDPR) derogations by including loopholes for political parties risk undermining the protections for personal data. GDPR is clear that derogations do not provide a 'free-for-all' for Member States, including in relation to exemptions and the processing of special category personal data. This flexibility has been interpreted as such, however, leading to the jarring outcome that certain national laws in this way invites data exploitation rather than data protection.

Despite concerns raised by civil society during the passage of national legislation – and since – there are loopholes for political parties included in, at least, the Spanish, Romanian and UK laws implementing the GDPR derogations.

In February, a Romanian civil society organisation, the Association for Technology and Internet (ApTI) complained[2] to the EU Commission. ApTI called on the EU Commission to review, among other matters, the provisions in the Romanian data protection law that allow political parties to process personal data from special categories without explicit consent and without implementing appropriate safeguards.

The Spanish law allows political parties to process personal data from publicly available sources. The Spanish Data Protection Authority (DPA) has been at pains to point out in an Opinion[3] published in December that this provision must be given a restrictive interpretation and should not be used for microtargeting. The Opinion sets out safeguards. It remains to be seen, however, the extent to which this Opinion will be followed in the run-up to elections and whether parties that fail to adhere will be held accountable.

National GDPR laws invite data exploitation rather than data protection.

The UK law permits political parties to process personal data "revealing political opinions" without the need for consent. This provision remains in the law despite concerns raised by Privacy International and others[4] during the passage of the Bill. The UK DPA, the Information Commissioners Office (ICO) has reported extensively[5] on the risks that the abuse of personal data pose for democracy and has recently consulted on a Code of Practice on the use of personal data in political campaigns.

In practice, meaningful data protection requires constant vigilance and enforcement. Legal loopholes make that even more challenging. Preferably, these exemptions for political parties would not have been passed into law. Still, where they have been, it is essential that DPAs give these provisions a restrictive interpretation, that political parties comply with this interpretation and that DPAs use their powers to audit and follow up to ensure compliance.

By Ailidh Callander, Privacy International

[1] https://privacyinternational.org/topics/data-and-elections

[2] https://www.apti.ro/sites/default/files/Complaint%20on%20Romanian%20implementation%20of%20the%20GDPR%20-%20ApTI.pdf-elections

[3] https://www.aepd.es/prensa/2018-12-19.html

[4] https://www.independent.co.uk/news/uk/politics/cambridge-analytica-uk-party-personal-voter-data-facebook-breach-conservatives-labour-a8269021.html

[5] https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/

[6] https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-views-code-of-practice-for-the-use-of-personal-information-in-political-campaigns/

Privacy policies for Internet of Things devices must comply with GDPR

Many Internet of Things (IoT) devices, such as smart speakers, lightbulbs, hubs and fridges, collect personal data. These devices are increasingly popular, leading to increasing interaction with General Data Protection Regulation (GDPR) provisions. The amount of control that people have over the data about them is, to a large extent, dependent on how well manufacturers inform the users about what data the devices collect, what the data is used for, and what the likely consequences for the users are.

As a case study of this, Open Rights Group recently worked with researchers at the London School of Economics to produce an unboxing video exploring one specific IoT product, "Sammy Screamer". Sammy Screamer is a connected motion alarm made by a company called BleepBleeps. You attach the device to a door, pushchair or bag, for example. Then if the device moves it sends a signal via Bluetooth to your phone. Your phone then notifies you that the device has moved – useful, for example, to know if your sleeping child has stirred or if someone has entered your home or taken your bag without permission.

One of the areas the video examines is privacy, and particularly the device's privacy policy documentation (this section starts at 2m 54s).

When you buy the device on the BleepBleeps website, there is a link to the company's privacy policy in the footer of that webpage. It is unclear whether the contents of that privacy policy cover a) the BleepBleeps website, b) the device you are buying and its associated app, or c) both the website and the device/app.

If you received the device as a gift, you would not have seen the website link at all. When you receive the device, the box does not come either with a privacy policy in paper form or any link to a digitally-located privacy policy.

The only time a user sees a link to the BleepBleeps privacy policy is in the sign-up phase when setting up the app which links their phone with the motion alarm device.

You cannot use the device unless you sign up through the app. You cannot sign up without (silently) agreeing to the privacy policy. This is problematic, given that this type of implied consent is ruled out by GDPR.

The text linking to the privacy policy is incredibly small which means it is difficult to read and accurately tap on. It is also very easy to miss that text at the bottom of the screen.

This is only one short case study illustrating how people are expected to interact with an IoT device and where the shortfalls are in terms of GDPR. IoT device manufacturers should be making it easy for users to understand what data about them will be collected and how it will be used. They should also ensure that users are giving "freely given, specific, informed and unambiguous" consent rather than relying on silent, implied consent.

By Ed Johnson-Williams, Policy and Research Officer, Open Rights Group

Uber drivers demand their data

Four Uber drivers in the United Kingdom have initiated legal action under the General Data Protection Regulation (GDPR) to require that the company provide data it holds about them.

This case is a test for how the GDPR applies to gig economy workers. The drivers argue that they have a legal right as data subjects to all information that Uber holds about them, even where this is information that the company uses to run its business – such as algorithms.

The drivers want to know how Uber applies its algorithms to assign them jobs, and to get a precise measure of the time they spend working for the platform. This will enable them to accurately calculate holiday and other pay owed. They also want other data including passenger ratings, which will assist them to appeal any unfair dismissals from the app.

When the drivers asked Uber for this information directly, Uber provided a limited dataset which the drivers say is insufficient. Uber, however, has obligations of privacy too, which may conflict with its obligations to disclose data, and it has intellectual property rights, which may allow it to withhold some confidential business information.

The drivers are represented by Ravi Naik of ITN Solicitors.

New evidence in AdTech complaint

Additional evidence has been supplied to data protection regulators in relation to a complaint about real-time bidding in the AdTech industry.

The evidence shows that the Interactive Advertising Bureau (IAB), an industry rule-setting body, knew that real-time bidding would be incompatible with General Data Protection Regulation (GDPR) requirements.

Complaints about the AdTech industry have been filed with Data Protection Authorities (DPAs) in the UK, Ireland and Poland.

More information is available at https://brave.com/update-on-gdpr-complaint-rtb-ad-auctions/

EDPB: e-Privacy and GDPR work together to protect people's data

The General Data Protection Regulation (GDPR) is very closely linked to other EU legislation protecting privacy of electronic communications ("e-Privacy"). A recent opinion[1] issued by the European Data Protection Board (EDPB) states authoritatively that GDPR and e-Privacy rules work together to provide comprehensive data protection.

This opinion refers formally to the 2002 Directive on Privacy and Electronic Communications, but it is issued without prejudice to the e-Privacy Regulation currently making its way through the European legislative process.

Progress on the e-Privacy Regulation has been rocky. It covers some of the most hotly contested areas in modern privacy and the digital economy, including online advertising, marketing and cookies, confidentiality of online communications in relation to traditional telecommunications and the privacy of smartphones and other devices, including apps. As such, it has been subjected to an unprecedented level of lobbying[2] by businesses concerned about consumers being given more power to control their data. This pressure has at times threatened to derail the entire process.

One of the points of contention is the relationship between e-Privacy and the GDPR. Some business lobbies have argued that there is no need to have two pieces of legislation as this creates conflicting[3] privacy safeguards. This contention has been contested[4] by the European Data Protection Supervisor (EDPS) in a lengthy piece advocating strongly for a reform of the current e-Privacy legislation. It has also been analytically critiqued in the EDPB's Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.

The EDPB Opinion was issued in response to a request from the Belgian Data Protection Authority (DPA) to clarify the interplay between e-Privacy and the GDPR. The main question asked by Belgium was whether national DPAs must or should take into account provisions of the e-Privacy Directive in their analysis and rulings. The EDPB was also asked to examine whether the "cooperation and consistency" mechanisms between DPAs can be engaged where processing can be governed by provisions of both the e-Privacy Directive and the GDPR.

The Opinion made it clear that both pieces of legislation are necessary. In some situations, only the GDPR will apply. In other situations, both the GDPR and e-Privacy laws can apply. Sometimes, e-Privacy goes further than the GDPR; for example, by protecting the legitimate interests of legal persons in addition to the fundamental rights of natural persons. A number of provisions in the e-Privacy Directive also "particularise and complement" the GDPR. In line with the standard rule that specific law trumps general law, where e-Privacy makes GDPR rules more specific, e-Privacy should prevail. For example, where e-Privacy stipulates that consent is required for a specific data processing activity, this will override the full range of possible lawful grounds for processing provided by Article 6 of the GDPR. This would be the case in most electronic communications and online marketing.

the e-Privacy Regulation has been subjected to an unprecedented level of lobbying by businesses concerned about consumers being given more power to control their data.

There are points where e-Privacy and the GDPR contain parallel obligations, for example to notify the relevant authorities of personal data breaches. The EDPB Opinion confirms that having regard to both pieces of legislation should not impose additional obligations or unnecessary administrative burdens. So, for example, breach notification need only be done once.

In terms of consistency and cooperation mechanisms, the EDPB confirmed that national DPA powers derive from the GDPR; they do not have automatic competency to enforce e-Privacy. DPAs need to be given specific powers or assigned tasks in order to scrutinise data processing operations governed by e-Privacy law. States may also or alternatively appoint another authority or body as an e-Privacy enforcement authority. This has a range of possible implications[5], particularly in terms of fine levels.

In issuing this Opinion, the EDPB seems to be losing patience with European legislators who are stalling in taking the e-Privacy Regulation forward. The day after publishing the Opinion, the EDPB issued a further statement[6] calling for stronger efforts to be made towards the adoption of an e-Privacy Regulation and urging legislators to start trilogue negotiations as soon as possible. It stated that the Regulation "must complement the GDPR by providing additional strong guarantees for all types of electronic communications." Apparently concerned about the potential for watering down the provisions by the Council of the European Union, the EDPB also insisted that "the e-Privacy Regulation must under no circumstances lower the level of protection offered by the current e-Privacy Directive."

By Javier Ruiz, Policy Director, Open Rights Group

[1] https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy-directive_en
[2] https://dma.org.uk/article/what-happened-to-the-eprivacy-regulation
[3] https://www.euractiv.com/section/data-protection/news/industry-groups-amp-up-lobby-campaign-to-topple-eprivacy-bill/
[4] https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en
[5] https://www.out-law.com/en/articles/2019/March/gdpr-e-privacy-breaches-factored-into-fines/
[6] https://edpb.europa.eu/sites/edpb/files/files/file1/201903_edpb_statement_eprivacyregulation_en.pdf

German competition regulator demands changes to Facebook's use of personal data

Authorities in Europe have for years discussed in theory the need to integrate data protection with consumer rights and competition law. This is the "holy trinity" required to properly protect citizens from the risks created by new technologies such as big data and machine learning. Practical progress on this integration has been slow. However, a critical new development in Germany hints that this may be about to change.

In February 2019, Germany's national competition regulator, the *Bundeskartellamt*, concluded[1] a three-year investigation into Facebook's use of personal data and ordered the company to change its data practices for German users. The investigation and ruling marks a huge step forward for using data protection law as a standard to examine and address exploitative practices by large internet companies.

The competition authority's investigation focused on Facebook's terms and conditions, which enable Facebook to collect and combine user data from third-party websites and apps into the platform even where users set their internet browsers to block activity tracking. It questioned whether these terms are unfair or violate data protection provisions including the General Data Protection Regulation (GDPR), and whether this unfair or illegal data collection constitutes an abuse of dominance in the social networks market.

The Bundeskartellamt found that Facebook's terms are contrary to data protection law as they enable Facebook to collect an almost unlimited amount of personal data from third-party sources without genuine user consent. Personal data flows automatically to Facebook whenever a user opens a web-page that has a visible Facebook plugin or that uses Facebook Analytics as a background service. Facebook users cannot opt out of this data collection and subsequent use but are instead forced to agree to the practice in order to access the platform.

The Bundeskartellamt also found that the extent to which Facebook collects, merges and uses data in user accounts amounts to an abuse of the social network's market dominance. This was a particularly innovative finding. Before this investigation, the market category of "social networks" had not been defined nor analysed. Instead, competition authorities assessing, for example, mergers simply considered Facebook's fiscal share of the overall advertising market, which has typically let the company off the hook for its shady data processing activities.

The Bundeskartellamt found that Facebook's terms are contrary to data protection law as they enable Facebook to collect an almost unlimited amount of personal data from third-party sources without genuine user consent.

The ruling sends a powerful signal to Facebook that it is not beyond the reach of competition authorities' jurisdiction. It could set an important precedent[2] for other European competition enforcers looking to use data privacy or consumer protection to pursue dominant data-collecting companies. It may even have influence further abroad, given Senator Elizabeth Warren's manifesto[3] in the United States presidential election campaign to break up big tech.

By Open Rights Group

[1] https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html

[2] https://www.bloomberg.com/news/articles/2019-02-07/facebook-ordered-to-change-user-data-policy-in-german-order-jruemcbm

[3] https://medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c

After Brexit, the EU must decide if UK data protection is adequate

Data protection is a core part of the European Union's Digital Single Market strategy. In many ways, the General Data Protection Regulation (GDPR) represents the EU's entire visionary future: a set of rules governing all Member States in a unified framework that facilitates ever closer operation.

For the United Kingdom (UK), however, it is Brexit rather than harmonised operation that draws ever closer. This brings one particular GDPR issue very much into the spotlight: on whatever basis and on whatever date the UK leaves the EU, an adequacy assessment will be required to maintain data flows. The European Commission will decide whether the UK provides equivalent data protection standards to GDPR and other EU legislation.

The adequacy assessment is going to be a key test of the UK's data privacy standards and achieving adequacy will be far from straightforward. The UK has committed to maintaining GDPR standards post-Brexit but this is not the whole picture for data protection compliance, and when it comes to the protection of fundamental rights there are difficult questions to be addressed.

First, although the UK theoretically already has a robust data protection framework very much aligned with the EU, there are derogations within the GDPR national implementing law (the Data Protection Act 2018) that may place adequacy at risk. Second, adequacy will scrutinise problematic areas such as national security arrangements that the UK has previously avoided having to defend. Third, the European Commission is not the sole arbiter in this area, and there may be stark differences of opinion between EU institutions that end up analysing the UK data protection regime.

In terms of UK law, the most troubling derogation from GDPR is an exemption from data protection rights where these would "prejudice … effective immigration control". This immigration exemption has been widely criticised[1] and is currently being challenged in the UK courts. Some critics have already pointed to[2] its potential implications for adequacy, and highlighted[3] that the adequacy assessment could conclude that it threatens fundamental rights to such an extent that it fails to provide "essentially equivalent" standards.

The UK's record on balancing national security against the right to privacy may also pose a problem for adequacy. The government has been castigated for its poor privacy protection by the European Courts in three significant cases in the past three decades, the most recent finding being late last year[4] when the mass surveillance programmes of government agency GCHQ revealed by Edward Snowden were found to be unlawful. This, together with the government's data-sharing arrangements between the so-called "Five Eyes", may hold back an adequacy ruling from the European Commission until necessary changes are made.

The adequacy assessment is going to be a key test of the UK's data privacy standards and achieving adequacy will be far from straightforward.

The European Commission, however, is not the only voice in the adequacy assessment. Just ask the United States. In 2000, the Safe Harbor framework, a system of rules allowing large data controllers based in the US such as Amazon, Facebook, Google and Microsoft to self-certify as "adequate" was given the green light by the European Commission. This framework was swiftly challenged[5] by privacy advocate Max Schrems in the European Court of Justice, and brought down on the basis that the framework did not in fact provide "essentially equivalent" standards of protection. The lesson the UK should take from this is that even if you smoothly achieve adequacy via the Commission, all it takes is a plucky law student from a Member State to start creating problems.

Data flows are an incredibly important part of the UK's economy and security and the digital exchanges between the UK and the EU are mutually beneficial. But there'll be no "free pass" for the UK from the Commission on adequacy. The UK will and should be subjected to the same high level of scrutiny as any third-party country. Failing to do so would set a bad precedent and might lock the process into perennial legal challenges.

Although rhetoric around Brexit has prominently touted the notion of "taking back control", adequacy ties the UK to EU standards. The UK may constitutionally reject the vision of ever closer operation, but however Brexit pans out, the influence of the Union and its institutions and the standards set by GDPR are going to have to be recognised and responded to by the UK for years to come.

By Open Rights Group

[1] https://www.theregister.co.uk/2018/03/05/uk_government_legal_challenge_immigration_exemption_data_protection_bill/

[2] https://www.theregister.co.uk/2018/03/07/mp_debate_commons_data_protection_bill_second_reading_immigration_exemption_press_regulation/

[3] https://iapp.org/news/a/will-the-uk-achieve-adequacy-after-brexit-even-the-ico-isnt-so-sure/

[4] https://techcrunch.com/2018/09/13/uks-mass-surveillance-regime-violated-human-rights-law-finds-echr/

[5] https://www.businessinsider.com/ecj-safe-harbor-ruling-bots-expected-2015-10?r=US&IR=T

EDPS 2018 Annual Report highlights the power and limitation of data protection

In February 2019, the European Data Protection Supervisor (EDPS), Giovanni Buttarelli, published his first Annual Report[1]. For those working on or interested in data protection, this 73-page (plus Annexes) report is well worth reading in full. It contains a comprehensive account of the EDPS office's activities across the remit of its mandate and provides a useful guide as to where 2019 interests and priorities lie.

The EDPS office was impressively active in 2018; the report details a full programme of operations which post-May included extensive work around getting the EU up-to-speed following the regime changes brought in by GDPR.

GDPR seems to have had a generally positive impact on the work of the EDPS, particularly in empowering individual complaints and enabling the office to push more strongly for data protection accountability in the EU institutions. Oddly, however, the report opens with the less-than-optimistic statement that *"2018 demonstrated the power and the limitations of data protection."* There's a striking discord between the report's substantive content, which details confidently the action taken to prepare, train and equip EU institutions and bodies to comply with the new data protection regime, and the despondency expressed in the foreword that this same regime is insufficient to adequately protect privacy.

The foreword's attitude towards GDPR contrasts starkly with the privacy and data protection improvements the EDPS celebrates having made through its activities. It also sits oddly alongside a stated 2019 objective to develop a framework for the EU institutions to proactively implement data protection safeguards into EU policy. Buttarelli lauds the leading role the EU institutions take in their implementation of GDPR rules but in the same breath fatalistically comments that this system of data protection is inherently susceptible to both data breaches and political manipulation.

Misuse of personal data for commercial and political purposes was the issue which dominated data protection discourse in 2018.

When launching the report, Buttarelli's press release said; *"Public awareness about the value of **online privacy** is at an all time high, while concern about the **abuse of personal data** by online service providers remains a topic of enquiry for governments around the world"* (bold in original). Misuse of personal data for commercial and political purposes was the issue which dominated data protection discourse in 2018. The EDPS Opinion on online manipulation and personal data[2] – one of 11 published during the year – concluded that regulators including competition authorities and election monitors urgently needed to collaborate to tackle localised and structural abuses. Perhaps Buttarelli's rather negative commentary stems from this point – although the Opinion was drafted in March 2018, GDPR seems to have had little impact on resolving this "worsening" issue.

Despite his comments, it is clear that as Buttarelli concludes his mandate in 2019 he is full of energy to do more. One thing that stands out in the report is how particularly proud he is of his actions in driving digital ethics onto the global agenda: the report comments multiple times on this workstream and details prominently the content and impact of the October 2018 International Conference of Data Protection and Privacy Commissioners. With clear momentum building, this is a topic on which the EDPS will focus heavily during 2019.

GDPR also infuses the other issues on the EDPS's 2019 agenda. The report mentions the forthcoming ePrivacy Regulation several times, and strongly urges its passing before the end of the current Parliamentary mandate. It indicates plans to conduct more investigation into data privacy issues around blockchain, press forward with an agenda of 'digital privacy by design' and reflect in a June 2019 report on the future of data protection within the EU and globally. These are all things to watch: given that the EDPS office sits at the heart of and directs the EU institutions' data protection decisions, its actions and statements will have a major influence on how GDPR will continue to develop and apply.

NOTES:

Who is the EDPS?

The EDPS is the EU's independent data protection authority, tasked with ensuring that the EU institutions and bodies respect and comply with their data protection obligations, both in processing personal data and by integrating data protection into all new legislation, policy and international agreements.

What does the EDPS do?

The EDPS supervises and enforces EU-level compliance with data protection. Its activities include giving substantive advice to the EU institutions and bodies in relation to risky personal data processing operations, handling complaints, monitoring compliance through visits and inspections, issuing formal Opinions, Comments and Guidance, providing training and running events and communications.

Under GDPR, the EDPS also acts as secretariat to the European Data Protection Board (EDPB), which works to ensure the consistent application of the GDPR across the EU.

The EDPS takes an active role in monitoring technological developments and their impact on data protection and privacy. It promotes privacy engineering and cooperates with national data protection authorities to develop common options for data protection by design. In 2018, it issued a formal Opinion on Privacy by Design[3].

By Amy Shepherd, Legal & Policy Officer, Open Rights Group

[1] http://publications.europa.eu/webpub/edps/2018-edps-annual-report/en/
[2] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
[3] https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

GDPR Explained

The GDPR: Everything you wanted to know.

What is the GDPR? Who is it for? Why does it matter? How will it affect me or my business?

Read our FAQ to find out the answers to these questions and more.

https://gdprexplained.eu

Bits of Freedom Data Request Tool

Use Bits of Freedom's tool to exercise your rights!

My Data Done Right helps internet users submit access, correction, deletion, and transfer requests. Bits of Freedom has already collected the contact details of more than 1,000 companies and government institutions; and the list keeps growing. Users don't have to think about the wording of these requests, as the text is generated for them in a privacy-friendly way. Finally, the tool helps users keep track of their requests and compares their results with others who have made similar requests.

See www.mydatadoneright.eu for more information.

If you are interested in joining the project and using the tool in your own country, please contact Bits of Freedom directly.

Access Now Guide to Lawmakers on GDPR

Making data protection law well: lessons learned from GDPR.

In January 2018, Access Now published a comprehensive guide to assist lawmakers in the development of data protection laws around the world.

Read the dos and don'ts of data protection law-making. The guide is available in English and Spanish.

English: **https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf**

Spanish: **https://www.accessnow.org/cms/assets/uploads/2018/04/manual-de-proteccion-de-datos.pdf**

FREE online course to learn about the GDPR

Make GDPR work for you – Know your rights!

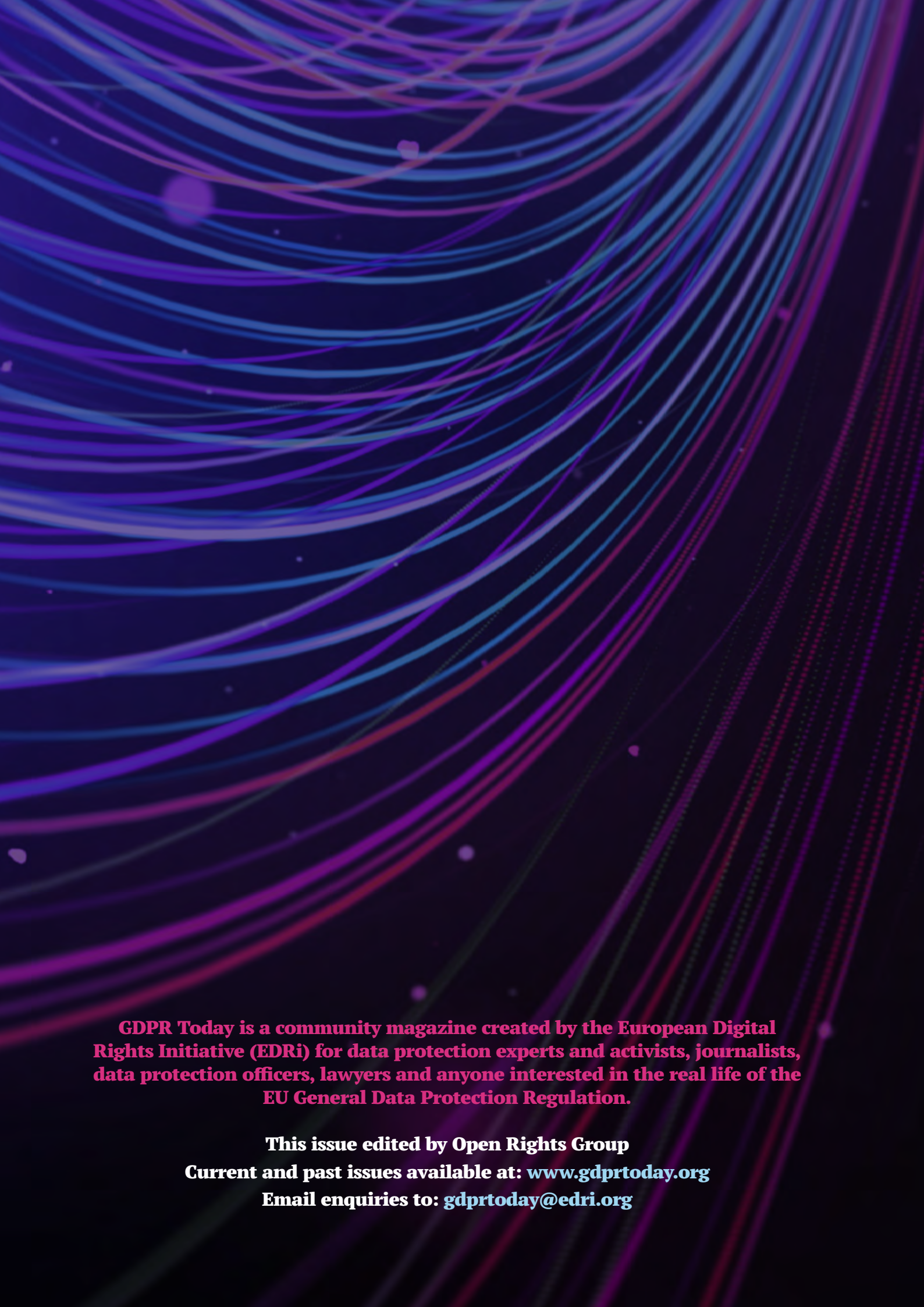
Do you want **more control** over your digital profile and reputation? Do you know your rights?

This **FREE online course** is your chance to learn new skills and significantly improve your digital life!

The course has been developed by digirights.info and is aimed at civil society organisations, activists, individuals and businesses.

For more information, see **https://digirights.info**

EU Member State	Office	Director/ President/ Chairperson	Email	Address
Austria	Österreichische Datenschutzbehörde	Mr Andrea JELINEK	dsb@dsb.gv.at	Barichgasse 40-42, 1030 Wien
Belgium	Autorité de la protection des données (APD-GBA)	Mr Willem DEBEUCKELAERE	contact@apd-gba.be	Rue de la Presse 35, 1000 Bruxelles
Bulgaria	Commission for Personal Data Protection	Mr Ventsislav KARADJOV	kzld@cpdp.bg	2, Prof. Tsvetan Lazarov blvd., Sofia 1592
Croatia	Croatian Personal Data Protection Agency	Mr Anto RAJKOVČA	azop@azop.hr	Martićeva 14, 10000 Zagreb
Cyprus	Office of the Commissioner for Personal Data Protection	Ms Irene Loizidou NIKOLAIDOU	commissioner@dataprotection.gov.cy	1 Iasonos Street, 1082 Nicosia / P.O. Box 23378, CY-1682 Nicosia
Czech Republic	Office for Personal Data Protection	Ms Ivana JANU	posta@uoou.cz	Pplk. Sochora 27, 170 00 Prague 7
Denmark	Datatilsynet	Ms Cristina Angela GULISANO	dt@datatilsynet.dk	Borgergade 28, 5
Estonia	Estonian DP Inspectorate	CURRENTLY VACANT	info@aki.ee	39 Tatari Street, 10134 Tallinn
Finland	Office of the Data Protection Ombudsman	Mr Reijo AARNIO	tietosuoja@om.fi	P.O. Box 800, FIN-00521 Helsinki
France	CNIL	Ms Marie-Laure DENIS		3 Place de Fontenoy, TSA 80715 – 75334 Paris, Cedex 07
Germany	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	Mr Ulrich KELBER	poststelle@bfdi.bund.de	Husarenstraße 30, 53117 Bonn
Greece	Hellenic DPA	Mr Konstantinos MENOUDAKOS	contact@dpa.gr	Kifisias Av. 1-3, PC 11523, Ampelokipi Athens
Hungary	National Authority for Data Protection and Freedom of Information	Dr Attila PéTERFALVI	peterfalvi.attila@naih.hu	Szilágyi Erzsébet fasor 22/C, H-1125 Budapest
Ireland	Data Protection Commissioner	Ms Helen DIXON	info@dataprotection.ie	21 Fitzwilliam Square, Dublin 2, D02 RD28
Italy	Garante per la protezione dei dati personali	Mr Antonello SORO	garante@garanteprivacy.it	Piazza di Monte Citorio, 121, 00186 Roma
Latvia	Data State Inspectorate	Ms Daiga AVDEJANOVA	info@dvi.gov.lv	Blaumana str. 11/13-15, 1011 Riga
Lithuania	State Data Protection Inspectorate	Mr Raimondas ANDRIJAUSKAS	ada@ada.lt	A. Juozapaviciaus str. 6, LT-09310 Vilnius
Luxembourg	Commission Nationale pour la Protection des Données	Ms Tine A. LARSEN	info@cnpd.lu	1, avenue du Rock'n'Roll, L-4361 Esch-sur-Alzette
Malta	Office of the Information and Data Protection Commissioner	Mr Saviour CACHIA	idpc.info@idpc.org.mt	Second Floor, Airways House, High Street, Sliema SLM 1549
Netherlands	Autoriteit Persoonsgegevens	Mr Aleid WOLFSEN		Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ Den Haag
Poland	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	Ms Edyta Bielak-JOMAA	kancelaria@uodo.gov.pl	ul. Stawki 2, 00-193 Warsaw
Portugal	Comissão Nacional de Protecção de Dados - CNPD	Ms Filipa CALVÃO	geral@cnpd.pt	Av. D. Carlos I, 134, 1º, 1200-651 Lisboa
Romania	The National Supervisory Authority for Personal Data Processing	Ms Ancuţa Gianina OPRE	anspdcp@dataprotection.ro	B-dul Magheru 28-30, Sector 1, BUCUREŞTI
Slovakia	Office for Personal Data Protection	Ms Soňa PŐTHEOVÁ	statny.dozor@pdp.gov.sk	Hraničná 12, 820 07 Bratislava 27
Slovenia	Information Commissioner	Ms Mojca PRELESNIK	gp.ip@ip-rs.si	Dunajska 22, 1000 Ljubljana
Spain	Agencia Española de Protección de Datos (AEPD)	Ms María del Mar España MARTI	internacional@agpd.es	C/Jorge Juan, 6, 28001 Madrid
Sweden	Datainspektionen	Ms Lena Lindgren SCHELIN	datainspektionen@datainspektionen.se	Drottninggatan 29, Box 8114, 104 20 Stockholm
UK	Information Commissioner's Office	Ms Elizabeth DENHAM	casework@ico.org.uk	Water Lane, Wycliffe House, Wilmslow, Cheshire SK9 5AF



GDPR Today is a community magazine created by the European Digital Rights Initiative (EDRi) for data protection experts and activists, journalists, data protection officers, lawyers and anyone interested in the real life of the EU General Data Protection Regulation.

This issue edited by Open Rights Group

Current and past issues available at: www.gdprtoday.org

Email enquiries to: gdprtoday@edri.org