

Open Rights Group submission to the call for evidence on the 'Impact of Covid-19 on DCMS sectors'

29 May 2020

S0. Executive summary

1. Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK.
2. This submission is in response to the Digital, Culture, Media and Sports Committee (DCMS) call for evidence about the impact of Covid-19 on any sectors under their remit. In particular, we answer to the question “What has been the immediate impact of Covid-19 on the sector?”, and on this basis we recommend the DCMS to take action.
3. We highlight the impact of COVID-19 on the Information Commissioner’s Office, and from that, on data protection enforcement in the private and public sector. COVID-19 has brought huge changes in the way data is being used by the Government and the private sector, which needs close scrutiny.
 - In section 1 (p.2), we analyse how the Information Commissioner’s Office (ICO) response to Coronavirus jeopardises its role of Supervisory Authority, by leaving it without effective investigative tools and, in turn, without the means to supervise and enforce the law.
 - In section 2 (pp. 3-4), we explain why this approach does not find any precedent in other agencies’ response to the Coronavirus crisis, whose approaches are diverse, yet directed toward ensuring continuity of their institutional role.
 - In section 3 (pp. 5-7), we demonstrate how this state of affairs has already resulted in tangible regulatory breaches, which constitute a material violation of individuals’ rights.
 - In section 4 (p.8), we outline our conclusions, and
 - In section 5 (p.8), we recommend that the Committee invites the ICO to a hearing, in order that they clarify their policy and, most importantly, demonstrate that they are capable of ensuring adequate regulatory oversight and enforcement.

S1. Data protection oversight under the lens

4. The Information Commissioner's Office (ICO) recently outlined its approach to face the Coronavirus pandemic.¹ Unfortunately, we find ICO's policy to be contradictory and, ultimately, ineffective.
5. In particular, ICO's official policy states that "We [the ICO] have stood down our audit work²". This policy is further substantiated as follows: "Due to Covid-19 the ICO will not be undertaking in-person/onsite audits for the foreseeable future".³
6. This needs to be read in conjunction with the 2018 Data Protection Act (DPA), which provides the ICO with two means of investigation: information notices (i.e. in-written requests for clarifications) and assessment notices (i.e. compulsory audits). Furthermore, the DPA empowers the ICO to issue enforcement notices, provided that the Commissioner is satisfied that the person has failed to respect DPA provisions,⁴ and that these facts can be substantiated.⁵
7. Having said that, by standing down their audit work, the ICO seems to be foregoing to their power to inspect suspected organisations (i.e. to issue assessment notices). Likewise, the effectiveness of information notices under these circumstances can be questioned: knowing that written requests would not be followed by onsite inspections, a targeted organisation could safely decide to provide false or incomplete information to the ICO, thus eluding the only investigatory power they have decided to rely on.
8. Indeed, the ICO recently hit the news for telling complainants that they have "decided not to take forward any complaints that require organisations to take action or respond to enquiries"⁶. This seems to corroborate that the ICO would have deprived themselves of effective investigatory means, to the point that the most reasonable course of action is inactivity. Also, while the ICO have stated to us that "far fewer cases than we anticipated have been suspended and we have continued to work with organisations to investigate and make decisions on thousands of cases during the lockdown", it remains unclear what the true impact is. Furthermore their response to us does not address the impact of standing down auditing.⁷
9. Finally, the ICO's stand down comes in conjunction with a General Stay of the Information Tribunal:⁸ the result is that both regulatory and judicial oversight in the field of data protection are currently suspended, leaving individuals without any protection against unlawful uses of their personal data.

1 See the ICO Blog: *Information Commissioner sets out new priorities for UK data protection during COVID-19 and beyond*. Retrieved at <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/05/new-priorities-for-uk-data-protection-during-covid-19-and-beyond/>

2 See *The ICO's regulatory approach during the coronavirus public health emergency*, point 4 p. 4. Retrieved at <https://ico.org.uk/media/about-the-ico/policies-and-procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf>

3 Source: <https://ico.org.uk/for-organisations/audits/>

4 Section 149(1)

5 Section 150(1)

6 See WIRED *It looks like the UK's data regulator has given up, blaming coronavirus*. Retrieved at <https://www.wired.co.uk/article/ico-data-protection-coronavirus>

7 Email from James Moss, Acting General Counsel, ICO, to Jim Killock, 2 June 2020. In the Author's possession.

8 Source: <https://www.judiciary.uk/wp-content/uploads/2020/05/Stay-of-270420.pdf>

S2. Comparing the ICO stand down with other regulatory authorities

10. We have compared the ICO's response to other public bodies approaches to face the pandemic, either domestically or from overseas. Both comparisons have been conducted on samples of relevant organisations, by relying on publicly available information. Thus, this is not meant to be an exhaustive analysis, but rather an attempt to highlight the anomaly of ICO's approach. The full results of our mapping can be found in the Annexes (pp. 9-12).

S2.1 Domestic comparison

11. We have compared ICO's regulatory approach with that of other 14 UK regulatory authorities, agencies or public bodies (agencies). We found that other agencies are tending towards business continuity, contrary to the ICO's example.
12. Of the 14 agencies we analysed, 11 adopted a policy directed toward either carrying on normal activities, or reassessing priorities without impacting regulatory oversight and enforcement. Another one (the National Cyber Security Centre) did not adopt any formal policy to face the crisis, although their work on the NHSX contact tracing app leaves little doubts about their overall business continuity.
13. Furthermore, we find evidence which supports the policy statements of these agencies: 9 out of 14 have either issued enforcement notices,⁹ launched investigations during the course of the pandemic,¹⁰ or are carrying out inspections.¹¹ Another 2 agencies are inviting the public to keep engaged, and send materials in the course of proceedings which started before the pandemic.¹²
14. This leaves us with only 2 out of 14 agencies which have reduced their operations, these being the CareQuality Committee and the HM Revenue and Customs. However, their behaviour is nowhere close to ICO's full halt(S1). In these two cases the HM Revenue and Customs keeps conducting remote inspections,¹³ while the CareQuality Commission has put forth an interim "emergency support framework" to compensate their inability to carry out onsite inspections.¹⁴

S2.2. Overseas comparison

15. We have compared ICO's activities during the past two months with that of other 12 European data protection authorities (DPAs). Although the pandemic has hit different countries at different moments, and Governments' responses have varied significantly. Despite these underlying differences, we find some clear trends which distinguish these DPAs' approaches from the ICO's.

9 Advertising Standards Authority, National Crime Agency, and Ofcom

10 Competition and Markets Authority, Financial Conducts Authority, and the Investigatory Powers Commissioners' Office

11 CareQuality Commission (interim approach), Environment Agency, HM Revenue and Customs (remotely only), and the Planning Inspectorate (remotely only)

12 British Board of Film Classification, and Ofgem

13 Source: <https://www.gov.uk/government/news/coronavirus-covid-19-update-on-voa-services>

14 Source: <https://www.cqc.org.uk/guidance-providers/how-we-inspect-regulate/emergency-support-framework-what-expect>

16. First of all, of the 12 DPAs we analysed, all have shown to be still actively enforcing data protection rules: 9 out of 12 have kept imposing fines,¹⁵ while the remaining three have kept processing complaints and issuing decisions.¹⁶ Furthermore, 6 DPAs have conducted inspections, or started new investigations or proceedings.¹⁷
17. Finally, the French DPA has shown a particularly proactive approach in scrutinising the development of the Contact Tracing App, e.g. by setting the terms for the implementation of IT systems to face the pandemic, and warning the Government about possible failures to comply with such terms.¹⁸ This is of particular relevance as France is among the few countries that, together with the UK, has opted to implement a centralised digital contact tracing system, whose invasiveness and security concerns are more acute.

15 Belgium, Croatia, Denmark, France, Greece, Hungary, Spain, Sweden, The Netherlands

16 Iceland, Italy, Poland

17 Denmark, France, Italy, Poland, Sweden, and the Netherlands

18 See *CNIL issues its guidance on the conditions to implement the application «Stop Covid»* [La CNIL rend son avis sur les conditions de mise en œuvre de l'application « StopCovid »]. Retrieved at <https://www.cnil.fr/fr/la-cnil-rend-son-avis-sur-les-conditions-de-mise-en-oeuvre-de-lapplication-stopcovid>

S3. Practical implications of ICO's stand down

18. On top of these issues, there is evidence that ICO's approach is falling short of addressing the needs and challenges resulting from the pandemic.
19. For instance, NHSX is planning to deploy a digital contact tracing solution. This is one among numerous initiatives to counter the spread of Coronavirus, whose reliance on sensitive health information makes the need for close and timely scrutiny self-explanatory. However, we have yet to see any action taken by the ICO to prevent or deal with a number of material breaches and abuses which have already taken place.

S3.1 Ascertained data breach

20. A contact tracing outsourcing firm has been the author of a serious data breach involving contact tracers' data, and yet deliberately decided not to refer its case to the ICO.¹⁹

S3.2 Contact Tracing App affected by security flaws

21. The NHSX has endangered people's right to privacy and data protection by distributing a Contact Tracing App affected by serious security flaws, as exposed by security experts²⁰ and confirmed by the NCSC.²¹
22. The NCSC justifies NHSX behaviour upon the basis that the Contact Tracing App would be in beta release (i.e. an application which still lacks maturity, and is distributed to the public for troubleshooting purposes). However, the NHSX website never identifies the app as in beta testing,²² nor any reference is to be found in the Google²³ or Apple²⁴ stores descriptions.
23. It follows that users were exposed to significant risks without being properly informed, in stark violation of GDPR principles of fairness, transparency, and security.²⁵ Also, this behaviour fundamentally undermines trust over the voluntary nature of the app: users were not given the opportunity to understand the implications of their choice, nor to cope with the security risks they were exposed to.
24. Finally, guidance concerning IT governance and management has already highlighted how using personal data in a testing environment should be avoided where possible, and otherwise be preceded by the explicit consent of the data subject.²⁶

19 "When the Home Office made a similar error last year it referred itself to the Information Commissioner, but Serco is not intending to do this." Source: <https://www.bbc.com/news/uk-52732818>

20 See *Security analysis of the NHS COVID-19 App*. Retrieved at: <https://www.stateofit.com/UKContactTracing/>

21 See NCSC *NHS Covid-19 app security: two weeks on*. Retrieved at: <https://www.ncsc.gov.uk/blog-post/nhs-covid-19-app-security-two-weeks-on>

22 Source: <https://covid19.nhs.uk/>

23 Source: <https://play.google.com/store/apps/details?id=uk.nhs.nhsx.colocate>

24 Source: <https://apps.apple.com/us/app/nhs-covid-19/id1507396059>

25 Article 5 letters a, f of Regulation (EU) 2016/679

26 See the European Data Protection Supervisor, *Guidelines on the protection of personal data in IT governance and IT management of EUIs*, §80, §82 p. 20. Retrieved at: https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf

S3.3 Lack of oversight over NHSX breach of GDPR rules

25. The NHSX will share contact tracing data with a number of private partners.²⁷ Furthermore, the NHS has been launching a number of projects regarding data analysis and research about Covid-19²⁸. In particular, we draw the attention to the Government practice of relying on a variety of data stores to enhance Covid-19 data,²⁹ as well as their plans to involve the innovation centre of the Ministry of Defence³⁰ in collecting “data from third party app-providers to help the NHS respond to the COVID-19 pandemic³¹”.
26. In this regard, the Data Protection Impact Assessment (DPIA) released by the NHSX identifies the legal basis to transfer contact tracing data to its partners in the COPI notices. However, COPI notices regulate the use of patients’ information by healthcare professionals,³² and are a substantially invalid ground for the processing of personal data by many NHSX partners. It follows that, in stark contravention of data protection laws, a suitable legal basis for these partners to use patients’ information is currently missing.
27. Also, the DPIA revealed the persistence of significant residual risks, which have not been mitigated. For instance, self-reporting has been widely recognised as a significant source of risk, which could lead to false alerts and scaremongering. Nevertheless, no measure to mitigate this risk has been provided in the DPIA, except for the duty to use the app correctly in the terms of service of the app.³³
28. A DPIA which lacks measures to sufficiently mitigate risks, as in this case, must be submitted to the ICO for prior consultation.³⁴ NHSX failure to do so puts them, once again, in contravention of data protection rules.
29. Finally, a similar pattern is emerging regarding the wider ‘test and trace’ programme. No Data protection Impact Assessment was released prior to the programme’s commencement, despite being legally necessary.³⁵ The privacy statement itself was in poor shape.³⁶ Worse still, clear security risks emerged which needed to be addressed.³⁷

27 See Matthehw Gould, *The power of data in a pandemic*. Retrieved at: <https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/>

28 See NHSX, *How data is supporting the COVID-19 response*. Retrieved at: <https://www.nhsx.nhs.uk/covid-19-response/data-and-information-governance/how-data-supporting-covid-19-response/>

29 Source: <https://data.england.nhs.uk/covid-19/>

30 Source: <https://www.gov.uk/government/organisations/jhub-defence-innovation/about>

31 See NHSX, *Project Oasis*. Retrieved at: <https://www.nhsx.nhs.uk/covid-19-response/data-and-information-governance/project-oasis/>

32 “No person shall process confidential patient information under these Regulations unless he is a health professional or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.” Source: Section 7 paragraph 2 of the The Health Service (Control of Patient Information) Regulations 2002

33 See Privacy Impact Assessment Risk Register, row 11. Retrieved at: <https://faq.covid19.nhs.uk/20200505a%20DPIA%20Risk%20Log%20Covid%20Proximity%20App.pdf>

34 Article 36(1), Regulation(EU) 2016/679 (i.e. the GDPR)

35 See Politico, *UK ‘test and trace’ service did not complete mandatory privacy checks*. Retrieved at: <https://www.politico.eu/article/uk-test-trace-privacy-data-impact-assesment/>

36 See The Telegraph, *NHS under fire for plans to store track and trace data for 20 years*. Retrieved at: <https://www.telegraph.co.uk/technology/2020/05/28/nhs-fire-plans-store-track-trace-data-20-years/>

37 See The Telegraph, *NHS contact tracing undermined by hackers sending fraudulent warnings to public*. Retrieved at: <https://www.telegraph.co.uk/news/2020/05/30/nhs-contact-tracing-undermined-hackers-sending-fraudulent-warnings/>

30. Unfortunately, ICO's follow up on 'test and trace' appears to be quite feeble, while we find no evidence to suggest that ICO is dealing with the other material breaches we highlighted (§20-28). Indeed, we have evidence of the contrary, as the ICO is refusing to keep the NHSX accountable for not having submitted the App's Data Protection Impact Assessment for prior consultation.³⁸

S3.4 New risks on the horizon

31. Finally, we want to draw the attention to the recent establishment of a new Biosecurity Centre,³⁹ whose role will be to conduct real-time analysis about infections outbreaks, and inform the Government public health responses.⁴⁰

32. In this regard, we also note that recent events in the United States have seen the repurposing of contact tracing technologies as surveillance tools, and their use to curb civil liberties.⁴¹

33. Thus, we cannot but stress the importance of close and effective scrutiny over the necessity of involving security agencies in a public health response, as well as the legal basis and safeguards which would underpin such disclosures and use of sensitive information. If the ICO were to fail again in upholding their role, the impact on public trust would be severe.⁴²

38 See ICO *Statement in response to media enquiries about the Data Protection Impact Assessment for the NHSX's trial of contact tracing app*. Retrieved at: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/05/dpia-for-the-nhsx-s-trial-of-contact-tracing-app/>

39 See Financial Times, *UK turns to counterterror chief to run Covid-19 risk hub*. Retrieved at: <https://www.ft.com/content/8a37555e-8c56-4828-9ddb-e60290e5977f>

See also The Guardian, *Senior counter-terror official put in charge of new UK biosecurity centre*. Retrieved at: <https://www.theguardian.com/world/2020/may/12/former-counter-terror-official-tom-hurd-put-in-charge-new-uk-biosecurity-centre-coronavirus>

40 Source: <https://www.instituteforgovernment.org.uk/explainers/joint-biosecurity-centre>

41 See Minnesota authorities have begun contact tracing arrestees from protests. Retrieved at: <https://twitter.com/i/events/1266773270939881472>

See also NBC News, *Minnesota Public Safety Commissioner John Harrington says they've begun contact tracing arrestees*. Source: <https://twitter.com/NBCNews/status/1266758240018276352>

42 "The trust element issue is critical if this is to work [...] It's about transparency - who will be able to access the data, what check and balances will there be". Source: <https://www.telegraph.co.uk/news/2020/05/24/test-trace-system-launch-without-app-amid-privacy-fears/>

S4. Conclusion

34. The ICO's response to the coronavirus crisis has proven ineffective. It does not only leave scope for widespread abuses and noncompliance with the rules, but also exposes individuals to serious harms to their privacy. In turn, we believe this may result in individuals' refusal to use the tools the Government is developing to counter the spread of the virus, which would ultimately endanger people's lives. Ultimately, we believe the ICO is contributing to the problem, rather than helping to deal with it.

S5. Recommendations to the Committee

1. The Committee should ask the Information Commissioner to a hearing.
2. The Committee should ask:
 - 2.1. What work the ICO's Office is doing;
 - 2.2. Why they have scaled down enforcement more than other agencies;
 - 2.3. Why other DPAs are able to investigate, when the ICO is not;
 - 2.4. How do they plan to cope with the negative consequences which may result from reduced oversight;
 - 2.5. Why the ICO has not taken over a more critical and proactive role with regard of the UK government, given the problems that have been raised with, for instance, the NHSX Tracking App;
 - 2.6. What other areas of concern the ICO has with Government use of data in the crisis, and how the ICO proposed to make their opinions heard;
 - 2.7. Whether the ICO is engaging with the "Biosecurity" Unit, or has any concerns about how personal data may be used;
 - 2.8. Whether the ICO will consider enforcement action against any government departments, or the NHS and so on, and in what circumstances.

ANNEX I – Domestic comparison

Authority's Name	Status	Notes	Source(s)
Advertising Standard Authority	Carries on	Issued an enforcement notice	https://www.asa.org.uk/news/advertising-iv-drips-coronavirus-covid-19.html
British Board of Film Classification	Carries on	In principle business as usual, but they recognise there could be some disruptions	https://www.bbfc.co.uk/about-bbfc/media-centre/bbfc-update-coronavirus https://www.cqc.org.uk/guidance-providers/all-services/coronavirus-covid-19-pandemic-information-providers
CareQuality Commission	Reduced	Some notification exemptions, possible delays in proceedings, inspections are suspended (but interim approach has been disposed)	https://www.cqc.org.uk/guidance-providers/notifications/notification-finder https://www.cqc.org.uk/guidance-providers/registration/register-cqc-new-provider https://www.cqc.org.uk/guidance-providers/how-we-inspect-regulate/emergency-support-framework-what-expect https://www.gov.uk/government/collections/cma-covid-19-response
Competition and Markets Authority	Intensified	Business as usual, coronavirus taskforce, launched investigation	https://www.gov.uk/government/news/cma-launches-covid-19-taskforce https://www.gov.uk/government/news/cma-investigates-misleading-online-reviews
Environment Agency	Carries on	Working from home but fully operational, carrying on inspections	https://www.gov.uk/government/news/environment-agency-operational-update-3-april-2020 https://www.fca.org.uk/news/speeches/fca-national-international-response-coronavirus-brexit https://www.fca.org.uk/news/statements/business-interruption-insurance-during-coronavirus
Financial Conduct Authority	Carries on	Old processes keep being handled, new priorities	https://www.fca.org.uk/news/press-releases/fca-confirms-measures-insurance-customers-coronavirus https://www.fca.org.uk/news/press-releases/fca-confirms-temporary-financial-relief-customers-impacted-coronavirus https://www.fca.org.uk/news/press-releases/fca-commences-civil-proceedings-relation-alleged-unauthorised-investment-advisers
HM Revenue & Customs	Reduced	Regulatory easing on some strictly defined areas, physical inspections have been stood down (but evidence is acquired remotely)	https://www.gov.uk/government/news/regulations-temporarily-suspended-to-fast-track-supplies-of-ppe-to-nhs-staff-and-protect-companies-hit-by-covid-19 https://www.gov.uk/government/news/coronavirus-covid-19-update-on-voa-services

Investigatory Powers Commissioners' Office	Intensified	Appointment of temporary judicial commissioners	https://www.ipco.org.uk/Default.aspx?mid=4.38
National Cyber Security Centre	Unknown	Seems business as usual	https://www.ncsc.gov.uk/news/ncsc-provide-expertise-nhs-covid-19-app https://www.gov.uk/government/news/coronavirus-covid-19-update-on-voa-services https://www.nationalcrimeagency.gov.uk/news/coronavirus-press-conference-25-april-2020-director-general-lynen-owen-s-speech
National Crime Agency	Carries on	Emphasis on business continuity, claims of intensifying efforts are not substantiated	https://www.nationalcrimeagency.gov.uk/news/millions-of-pounds-and-tonnes-of-drugs-seized-during-lockdown https://www.nationalcrimeagency.gov.uk/news/nca-recovers-8-million-linked-to-international-organised-crime
Ofcom	Carries on	Priority have been reassessed, but keeps issuing fines	https://www.ofcom.org.uk/about-ofcom/policies-and-guidelines/coronavirus-information https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/loveworld-breaks-broadcasting-rules-covid-19
Ofgem	Carries on	Delaying some consultation, otherwise not stopping their work	https://www.ofgem.gov.uk/publications-and-updates/ofgem-information-energy-licensees-coronavirus-covid-19-response
Planning Inspectorate	Carries on	Casework is processed online, inspections are carried out virtually	https://www.gov.uk/guidance/coronavirus-covid-19-planning-inspectorate-guidance https://www.gov.uk/government/news/planning-inspectorate-coronavirus-covid-19-update-16-april-2020
Security Industry Authority	Carries on	Keeps processing enquiries, working from home	https://www.sia.homeoffice.gov.uk/Pages/Coronavirus.aspx

ANNEX II – Overseas comparison

DPA	Activities	Evidence
Belgium	Previous consultation on contact tracing, imposed fines	<p>Previous Consultation https://www.autoriteprotectiondonnees.be/news/avis-de-l-APD-sur-arretes-royaux-relatifs-aux-applications-de-tracage-et-base-de-donnees-covid-19</p> <p>28.04 https://gdprhub.eu/index.php?title=APD/GBA_-_AH-2019-0013</p> <p>20.04 https://gdprhub.eu/index.php?title=APD/GBA_-_16/2020</p>
Croatia	Warned the Croatian Institute of Public Health about use of personal data, imposed fines	<p>Warning https://azop.hr/aktualno/detaljnije/obrada-osobnih-podataka-klijenata-u-usluznim-djelatnostima-u-kontekstu-covi</p> <p>13.03 https://gdprhub.eu/index.php?title=AZOP_-_credit_institution_decision</p>
Denmark	Several criticism, decisions and fines issued in the last two months	<p>Last Month Activities https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/</p> <p>27.05 https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/maj/ny-afgoerelse-manglende-opfyldelse-af-oplysningspligt/</p> <p>10.03 https://gdprhub.eu/index.php?title=Datatilsynet_-_To_kommuner_indstillet_til_b%C3%B8de</p>
France	Issued guidance on covidapp and scrutinises government adherence to the guidance, investigated on surveillance practices, and imposed fines	<p>Covid Guidance https://www.cnil.fr/la-cnil-rend-son-avis-sur-les-conditions-de-mise-en-oeuvre-de-lapplication-stopcovid</p> <p>Investigation https://www.cnil.fr/fr/suspension-de-lutilisation-des-drones-pour-controler-le-deconfinement-paris-par-le-conseil-de-tat-les</p> <p>27.03 https://gdprhub.eu/index.php?title=CE_-_N%C2%B0_431350</p>
Greece	Suspended public meetings, imposed fines	<p>Suspension https://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=99,127,162,122,146,188,11,200</p> <p>20.03 https://gdprhub.eu/index.php?title=HDPa_-_4/2020</p>
Hungary	Imposed a fine	<p>04.03 https://gdprhub.eu/index.php?title=NAIH_-_NAIH/2020/32/4</p> <p>13.05 https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_-_2020010598</p> <p>13.03 https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_-_2020010738</p>
Iceland	Imposed fines, processed complaints	<p>05.03 https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_-_2020010591</p> <p>05.03 https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_-_2020010428</p> <p>05.03 https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_-_2020010382</p>
Italy	Initiated an investigation on data breach, consulted about contact tracing legislation, processed complaints	<p>Investigation https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9304469</p> <p>Consultation https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9328050</p>

		23.03 https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_-_9304448
		Appointments https://uodo.gov.pl/138/1542
Poland	Still accepting to schedule appointments with complainants, investigating data breach, initiated and handled proceedings	Proceeding https://uodo.gov.pl/138/1526
		Data Breach https://uodo.gov.pl/138/1514
		06.04 https://gdprhub.eu/index.php?title=UODO_-_DS.523.1470.2020
Spain	Imposed a fine	19.03 https://gdprhub.eu/index.php?title=AEPD_-_PS-00008-2020
Sweden	Carried inspections, imposed fines	Inspection https://www.datainspektionen.se/nyheter/datainspektionen-inleder-granskning-av-kamerabevakning-i-hyreshus/
		11.05 https://gdprhub.eu/index.php?title=Datainspektionen_-_DI-2020-1539
The Netherlands	Started investigation, imposed fines	Investigation https://autoriteitpersoonsgegevens.nl/en/news/dutch-data-protection-authority-investigate-tiktok
		30.04 https://gdprhub.eu/index.php?title=AP_-_Fine_for_processing_employees%27_fingerprints