One-Stop-Shop Cross-Border Complaint Statistics

25 May 2018 - 19 Sept 2022

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Contents

EXECUTIVE SUMMARY

Since the introduction of the General Data Protection Regulation (GDPR) in May 2018, the Data Protection Commission (DPC) has received and concluded a significant number of cross-border complaints through the GDPR's "one-stop-shop" (OSS) mechanism.

This OSS innovation under the GDPR facilitates multi-national controllers that operate across the EU/EEA by allowing them deal with a single lead supervisory authority (LSA) as their "sole interlocutor". Only EU-based controllers or processors can qualify for the OSS. Whether to avail of it or not is a decision for the organisations themselves. This means many multi-nationals including large internet platform processing operations sit outside the OSS and, in those circumstances, any supervisory authority may be competent to act.

For any individual in an EU/EEA state, if they wish to lodge a complaint, they may lodge it directly with the supervisory authority that is the LSA (if there is an LSA) or they may lodge it with their local/national authority which will transmit it to the LSA if it transpires to be an "OSS case". Issues of language, translation and coordination arise in this process as well as, occasionally, displeasure on the part of some individuals when they discover that a draft of a GDPR Article 60 decision made in their case will be circulated across many EU/EEA data protection authorities. In such circumstances, the details of the individual are redacted or withheld when the draft decision is more widely circulated.

The European Data Protection Board (EDPB) is obliged to maintain a database of finalised cooperation and consistency decisions. However, as can be seen from a perusal of cases on the public register[1], not all authorities permit the EDPB to publish decisions and the database is not always up-to-date. Ex-officio or own-volition investigation decisions are also included on the EDPB database.

For the majority of cross-border complaints it receives, the DPC is responsible for dealing with them as the EU/EEA lead supervisory authority for the organisations concerned. The DPC also receives a number of complaints from individuals about organisations where another EU/EEA data protection authority is the lead. In these cases, the DPC transfers the complaints to the relevant authority via the OSS mechanism.

The DPC's handling of cross-border complaints continues to be the subject of public commentary, regrettably based on information that is incomplete and lacking context.

[1] https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en?f%5B0%5D=article_60_lsa%3A676

In the interests of accountability and transparency, in March 2022, the DPC published a report providing a detailed fact-based overview and statistical analysis of the DPC's handling of OSS complaints in the period May 2018 to end 2021.

This report updates the March 2022 publication with metrics and statistical analysis for the period 25 May 2018 to 19 September 2022. The report provides an overview of the cross-border complaint handling processes employed by the DPC and the associated metrics, including, the number of complaints received, numbers concluded, and outcomes achieved. For full context, the DPC has received almost 20,000 complaints since the GDPR came into application of which over 17,000 have been concluded.

The report illustrates that:

- **1,278 valid cross-border complaints have been received by the DPC; 1,091 (85%) as lead supervisory authority (LSA) and 187 (15%) as a concerned supervisory authority (CSA).**

- **678 (62%) cross-border complaints handled by the DPC as the LSA were originally lodged with another supervisory authority and transferred to the DPC.**

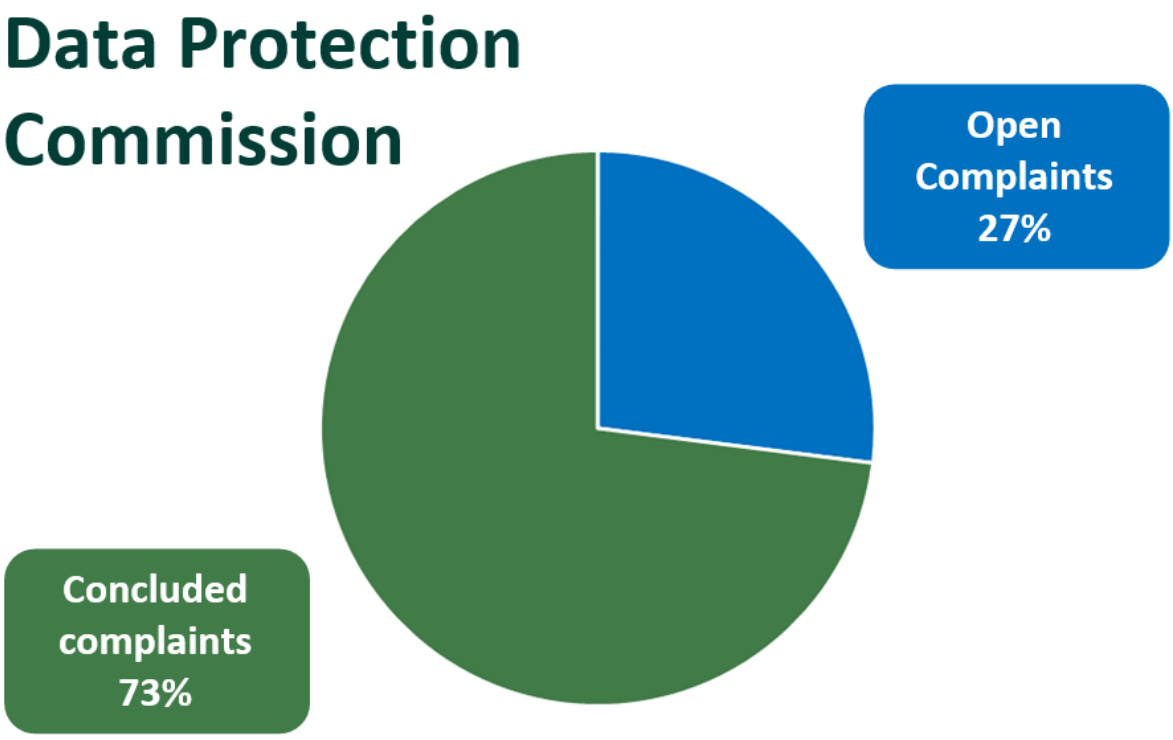
- **73% of all cross-border complaints handled by the DPC as the LSA since May 2018 have been concluded, with 88% of those received in 2018, 87% in 2019, 72% in 2020 and 52% in 2021 now concluded.**

- **Of the 798 concluded cross-border complaints handled by the DPC as the LSA, 659 (83%) were resolved through amicable resolution in the interests of the complainant.**

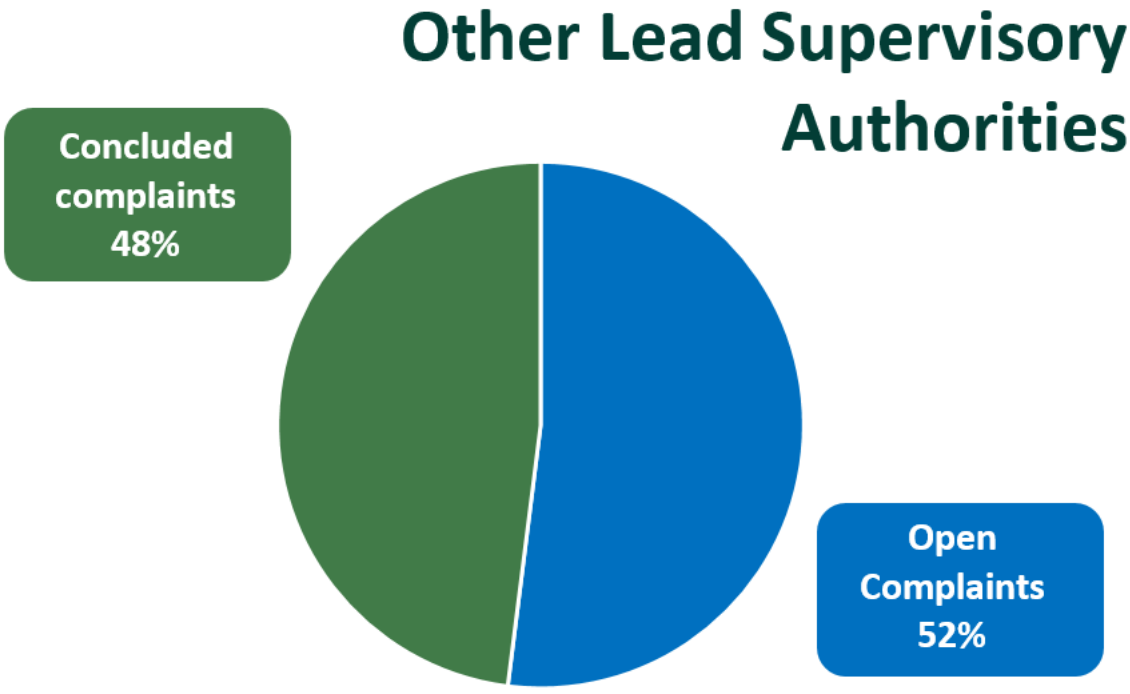
- **56 (19%) open cross-border complaints are linked to an inquiry and will be concluded on the finalisation of the inquiry. Over half of the remaining 71 open complaints from 2018 and 2019 are linked to an inquiry.**

- **87% of all cross-border complaints handled by the DPC as the LSA relate to just 10 data controllers.**

- **48% of complaints transferred by the DPC to other EU/EEA LSAs (excluding the UK) have been concluded.**



Cross-border complaints open and concluded where the DPC is the LSA



Cross-border complaints open and concluded where complaint lodged with the DPC and transferred to another EU/EEA authority (excl UK) as the LSA

ONE-STOP-SHOP MECHANISM – EU/EEA CROSS-BORDER COMPLAINTS

The GDPR which came into effect on 25 May 2018 provided for the creation of a new data protection regulation and enforcement system, called the "one-stop-shop" (OSS) mechanism. The fundamental purpose of this mechanism is to facilitate organisations who do business in more than one EU/EEA member state to engage with, and be subject to the regulatory supervision of, just one EU/EEA national data protection authority (referred to in the GDPR as a "supervisory authority"). The applicable supervisory authority will be that of the member state in which the organisation has based its "main or single establishment". This supervisory authority is referred to as the "lead supervisory authority" for that organisation. The one-stop-shop also enables individuals to lodge complaints with their local supervisory authority, which will then be transferred to the lead supervisory authority for assessment and resolution in cooperation with other supervisory authorities as required by the GDPR.

The main or single establishment of an organisation is generally its place of central administration and/or decision-making. As many of the major global multi-national technology and internet platform companies have based their European headquarters in Ireland, the DPC assumes the lead role in the assessment of the large number of complaints relating to cross-border processing[2] (cross-border complaints) by these companies, lodged by individuals across all 30 EU/EEA countries. This is clearly borne out by the statistics (see below) which show that of the **1,278 cross-border complaints received by the DPC since May 2018, which after initial assessment and review were deemed to be valid[3], 85% (1,091) were cases in which the DPC was the lead supervisory authority.**

The GDPR's one-stop-shop system also provides for supervisory authorities, other than the lead, to be designated a "concerned" supervisory authority. A supervisory authority is deemed to be "concerned" with a case if the organisation (controller or processor) is established on the territory of the Member State of that supervisory authority; if data

[2] Article 4(23) Regulation (EU) 2016/679 (General Data Protection Regulation)
'cross-border processing' means either:
processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

[3] The DPC deems a cross-border complaint valid following the completion of a series of assessment measures including, but not limited to, confirmation that the processing in question is cross-border in nature and that the DPC is either Lead Supervisory Authority or a Concerned Supervisory Authority, verification that all necessary documents have been made available (further documents will be requested where applicable); verification that the data subject has contacted the data controller to exercise their rights, etc.

subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or if a complaint has been lodged with that supervisory authority.

Since May 2018, 187 valid cross-border complaints have been lodged with the DPC where the DPC acts as a concerned supervisory authority, i.e., another supervisory authority is the lead and is responsible for handling the complaint.

In practice, operating the one-stop-shop system means that the DPC will play an active role in cross-border cases when:

- Complaints have been lodged directly with the DPC and the data controller involved has its main or single establishment in Ireland – ***the DPC is the lead supervisory authority (LSA)***
- Complaints have been lodged with a supervisory authority in another member state and the data controller involved has its main or single establishment in Ireland – ***the DPC is the lead supervisory authority (LSA)***
- Complaints have been lodged directly with the DPC and the data controller involved has its main or single establishment in another member state and there is an Irish interest in the complaint handling, in line with the "concerned" criteria above – ***the DPC is a concerned supervisory authority (CSA)***

DPC ROLE	NO. OF VALID COMPLAINTS	%
LEAD SUPERVISORY AUTHORITY (LSA)	1,091	85%
CONCERNED SUPERVISORY AUTHORITY (CSA)	187	15%
TOTAL	**1,278**	

Figure 1. CROSS-BORDER COMPLAINTS WITH DPC IN ACTIVE ROLE (since May 2018)

CROSS-BORDER COMPLAINT ASSESSMENT AND HANDLING

Before a complaint lodged with the DPC can be deemed valid under the GDPR and admissible for progression to the cross-border complaint handling phase, it must be fully assessed to ensure that it meets a number of criteria, e.g. that it relates to a data protection issue (rather than, for example, a customer service or online content issue), that copies of all necessary documentation have been submitted. Then it must be determined whether the processing at issue is cross-border, whether it concerns the dropping of cookies regulated under e-privacy legislation for which there is no one-stop-shop, whether the DPC is acting as LSA or CSA and in some cases further information may be needed from the complainant or the data controller before a determination can be made on the admissibility of a complaint.

The DPC carries out this assessment exercise on all cross-border complaints received directly from individuals. This assessment is also carried out on cross-border complaints received by other EU supervisory authorities and transferred to the DPC through the European Data Protection Board's IMI communications system[4]. If a complaint progresses through the various assessment stages and is deemed valid, with the DPC confirmed as the competent lead supervisory authority, the individual complainant is provided an update on the status of their case and the complaint will then move to the DPC's complaint handling stage of the process.

[4] The IMI system is an information sharing tool and not a case management system. As such, the statistics generated from the IMI relate to notifications of procedures/workflows initiated by supervisory authorities under various headings. In addition, references to case register entries in EDPB IMI statistics do not have a 1-to-1 correlation to the number of cross-border complaints handled per country as multiple complaints may be included in one case register entry. For example, Company A may have two case registers where all complaints relating to data subject rights are added to one register and complaints relating to the principles of data protection are added to the other. This means that the number of case registers per supervisory authority does not represent the totality of cross-border complaints received in any given period or the total number of cases resolved and closed. Case registers are repositories and largely perpetual in nature, in essence a filing system, created for the purpose of transferring complaints to the Lead Supervisory Authority.

CROSS-BORDER COMPLAINTS WITH DPC AS LEAD SUPERVISORY AUTHORITY (LSA)

In the period May 2018 to September 2022, the DPC has acted as LSA for 1,091 valid complaints, of which 678 (62%) were lodged by complainants with another EU/EEA supervisory authority and transferred to the DPC via the OSS mechanism. 413 (38%) of cross-border complaints were lodged directly with the DPC.

METHOD OF RECEIPT	NO. OF COMPLAINTS	%
VALID COMPLAINTS LODGED DIRECTLY WITH THE DPC	413	38%
VALID COMPLAINTS LODGED WITH ANOTHER EU/EEA SA	678	62%
TOTAL	1,091	

Figure 2. INITIATION METHOD OF CROSS-BORDER COMPLAINTS WHERE DPC IS LSA

Of the 1,091 valid cross-border complaints for which the DPC is the LSA since May 2018, 73% have now been fully concluded. The rate of closure continues to increase, as illustrated in the table below. 88% of the complaints received in 2018, 87% of those received in 2019, 72% received in 2020 and 52% received in 2021 have now been concluded.

YEAR	NUMBER OF VALID CROSS-BORDER COMPLAINTS RECEIVED	NUMBER CONCLUDED AS AT 19/9/22	% CONCLUDED
2018 (May – Dec)	156	145	88%
2019	400	354	87%
2020	298	216	72%
2021	170	78	52%
2022	67	5	7%[5]
TOTAL	**1,091**	**798**	**73%**

Figure 3. BREAKDOWN OF CROSS-BORDER COMPLAINTS RECEIVED PER YEAR AND CONCLUDED

A large number of open complaints dating from 2018 and 2019 are linked to an inquiry. Further analysis at section "CROSS-BORDER COMPLAINTS LEADING TO INQUIRIES".

[5] On average, provided there are no other delays, when corresponding with a complainant in another Member State regarding their complaint (which must be done via the concerned supervisory authority using the IMI), it may take at least three months from the time the DPC uploads its correspondence to the IMI until the DPC receives a reply from the complainant. In some instances, the DPC may reach out to the complainant three or four times as part of the complaint handling process in an attempt to amicably resolve the complaint for the complainant. The length of time it takes to exchange correspondence through the IMI/OSS (the process of translation of correspondence into the language of the complainant and vice versa by the concerned supervisory authority being a significant factor) has a direct impact on the length of time it takes to progress complaints to a conclusion.

OUTCOME OF CONCLUDED COMPLAINTS WHERE THE DPC IS LSA

There are various sets of circumstances and courses of action that can lead to the closure of a valid cross-border complaint by the DPC.

Concluded by Amicable Resolution

The first action taken by the DPC when it commences work on a valid cross-border complaint is to exercise the ***amicable resolution*** powers afforded to it by the Data Protection Act 2018[6]. The DPC will carry out an assessment of each valid cross-border complaint to establish if it is suitable for progressing with this, less adversarial, course of action designed to achieve speedier and more resource efficient outcomes for individuals. Amicable resolution involves contacting the organisation (data controller), asking questions in relation to the subject matter of the complaint, probing the answers provided by the organisation prior to proposing an amicable resolution to the complainant if the DPC is of the view that the responses of the organisation may facilitate an outcome in the interests of the complainant.

In reaching an amicable resolution, where the complaint was lodged with another supervisory authority, all communications from the DPC to the complainant are issued by that authority and both authorities cooperate to the extent required to progress the handling of the complaint.

Some examples of complaints which are often suitable for amicable resolution are access requests for personal data from online service providers, requests for the information required to access personal online accounts and requests for the erasure of personal data. Examples of complaints that prove difficult to amicably resolve relate to cases involving suspended accounts of individuals deemed to have breached a platform's community standards given that the central concern of the individual may truly be the loss of access to their account rather than a data protection issue *per se* . Other issues that prove challenging under GDPR relate to disputed content in the form of posts of photos and videos and comments (which is undoubtedly personal data in the cases presented to the DPC) but which has been generated, often by a "friend" of the complainant, and, in these cases, one of the questions that arises is, is it the role of the platform to censor the content posted by the "friend"?

Amicable resolution is an effective and important tool that the GDPR and the Data Protection Act 2018 provide for and which the DPC uses to reach outcomes in the best

[6] Section 109(2) of the Data Protection Act 2018:
"The Commission, where it considers that there is a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint, may take such steps as it considers appropriate to arrange or facilitate such an amicable resolution."

interest of complainants. **Of the 798 cross-border complaints (where the DPC is LSA) concluded in the period May 2018 to September 2022, 659 (83%) were closed through the amicable resolution process.**

Where an amicable resolution is successfully achieved, a complaint will be deemed to be withdrawn, in accordance with Section 109(3) of the Act [7].

Case studies which illustrate the effective use of the amicable resolution mechanism in achieving outcomes for complainants can be found at Appendix 1.

It should be noted, however, that there is **no obligation on complainants to agree to follow an amicable resolution** path once it has been proposed to them. Even in circumstances where the DPC considers that an amicable resolution is suitable and possible, and where it has conducted an investigation in furtherance of achieving an amicable resolution, the complainant can decide **not to accept it**. In these cases, which are in the minority due to the amount of work and resource put into proposing an appropriate amicable resolution to the complainant, the DPC will proceed to prepare a draft decision in accordance with Article 60 of the GDPR that will determine whether an infringement has taken place, and if any corrective powers are to be utilised.

Complainant no longer pursuing complaint

In some cross-border complaint cases, events occur which result in the complainant ceasing to engage with the DPC, even after their complaint has been accepted as valid. The reasons for this observed by the DPC range from the data controller having engaged with the complainant directly to resolve the issue without further involvement of the DPC, or the lack of a response from the complainant to a request for additional information which is necessary to proceed with the complaint. This trend also occurs when the DPC is handling national (or domestic as distinct from cross-border) complaints and, while there are many possible reasons, most likely that the matter has been resolved, the DPC must deem these complaints closed if engagement by the complainant with the DPC in relation to their complaint ceases. While no further action on the part of the DPC will take place in those circumstances, **the DPC will always re-open such complaints if the complainant decides at a future date to re-engage with the complaint handling process**.

[7] Section 109(3) of the Data Protection Act 2018:
"Where the parties concerned reach an amicable resolution of the subject matter of the complaint, the complaint shall, from the date on which the amicable resolution is reached, be deemed to have been withdrawn by the complainant concerned."

Of the 798 cross-border complaints (where the DPC is LSA) concluded in the period May 2018 to September 2022, 119 (15%) were closed on the basis that the complainant was no longer pursuing the complaint.

Article 60

As already referenced, the GDPR provides for the prospect of amicable resolution of complaints as an effective and efficient outcome for individuals. Having regard to the EDPB's guidelines on amicable settlements finalised in November 2021, these outcomes are also now detailed and recorded on the EDPB's information sharing platform (IMI). Equally, complaints that affect more than one individual or where an individual is not satisfied with the actions of the controller to resolve their complaint, may require further inquiry.

In total, to date, the DPC has concluded **89 cases** under the EDPB's guidelines for **Article 60 draft decisions.** A large number of further DPC inquiries have now reached a very advanced stage in the preparation of draft decisions for the Article 60 procedure. Further detail on the status of these inquiries is provided in the DPC's Annual Report for 2021 (pages 60 – 64)[8].

[8] https://www.dataprotection.ie/sites/default/files/uploads/2022-02/Data%20Protection%20Commision%20AR%202021%20English%20FINAL_0.pdf

CROSS-BORDER COMPLAINTS LEADING TO INQUIRIES

The DPC exercises its powers under the GDPR and the Data Protection Act 2018 to carry out inquiries into organisations where a potential significant risk to EU data subjects is in question. The DPC can commence a "**complaint based inquiry"** specific to an individual complaint. Alternatively, where there are multiple complaints pointing to potential systemic issues of non-compliance, the DPC may launch an **"own volition inquiry"** to investigate the matters concerned. In such circumstances, the DPC may pause the handling of the relevant individual complaints. The outcome of those complaints will remain pending until the related inquiry has been concluded, after which the handling of the related complaint will resume and be concluded on the basis of the DPC's decision in the own volition inquiry. This is an important DPC procedure and was central to the route followed in reaching the final decision in the WhatsApp own volition inquiry[9], in respect of which there were 30 individual linked complaints.

As at September 2022, 19% of open cross-border complaints were linked to an inquiry.

YEAR	NUMBER OF VALID CROSS-BORDER COMPLAINTS RECEIVED	NUMBER OF COMPLAINTS OPEN AT END AUGUST 2022	NUMBER OF OPEN COMPLAINTS LINKED TO AN INQUIRY	% OF OPEN COMPLAINTS LINKED TO AN INQUIRY
2018	156	18	13	72%
2019	400	53	26	49%
2020	298	83	14	17%
2021	170	82	3	4%
2022	67	62		0%
Total	**1,091**	**298**	**56**	**19%**

Figure 4. BREAKDOWN OF OPEN CROSS-BORDER COMPLAINTS LINKED TO AN INQUIRY

[9] https://www.dataprotection.ie/en/dpc-guidance/law/decisions/whatsapp-ireland-ltd-august-2021-0

CROSS-BORDER COMPLAINTS LODGED WITH OTHER SUPERVISORY AUTHORITIES

The GDPR One-Stop-Shop mechanism enables citizens to lodge complaints with their local supervisory authority, regardless of whether the data controller/processor has an establishment in that Member State. The DPC, therefore, receives complaints that have been lodged with all other EU/EEA supervisory authorities, for which it must handle as the lead supervisory authority. In these cases, all communication that the DPC has with the data subject in relation to their complaint is issued by the DPC through the relevant supervisory authority, whether that is a request for further documentation in relation to the complaint, proposals in relation to amicable resolution or correspondence relating to the Article 60 decision-making process.

The table below sets out the supervisory authorities from which the largest number of valid cross-border complaints were received in the period May 2018 to September 2022 (with DPC as LSA). The table also shows the percentage number of transmitted complaints concluded at the end of 2021. For example, valid cross-border complaints lodged with supervisory authorities in Germany account for 19% of all cross-border complaints handled by the DPC between May 2018 and September 2022. 74% of complaints received from Germany have been concluded.

COUNTRY (TOP 10)	% OF TOTAL VALID COMPLAINTS RECEIVED MAY 2018 TO 19/9/22	% OF COMPLAINTS CONCLUDED AT 19/9/22
Germany (Federal & Lander)	19%	74%
France	9%	51%
United Kingdom	8%	100%
Spain	7%	55%
Austria	4%	70%
Poland	3%	52%
Netherlands	2%	65%
Denmark	2%	55%
Italy	1%	50%
Belgium	1%	45%
Remaining 19 EU/EAA countries	9%	68%

Figure 5. % OF VALID CROSS-BORDER COMPLAINTS RECEIVED AND CONCLUDED PER INITIATING AUTHORITY

CROSS-BORDER COMPLAINTS BY ORGANISATION

The 1,091 valid cross-border complaints received since May 2018, for which the DPC is the LSA, involve over 75 different data controllers. The table below illustrates that 10 technology and internet platform multi-national companies account for 87% of complaints.

DATA CONTROLLER (TOP 10)	% OF TOTAL CROSS-BORDER COMPLAINTS DPC AS LSA
Meta Platforms Ireland Limited	31%
Google Ireland Limited	11%
WhatsApp Ireland Limited	8%
Airbnb Ireland UC	8%
Yahoo EMEA Limited	8%
Twitter International Company	5%
Microsoft Ireland Operations Limited	5%
Apple Distribution International	4%
MTCH Technology Services Limited	4%
LinkedIn Ireland UC	3%
	87%

Figure 6. % OF CROSS-BORDER COMPLAINTS PER DATA CONTROLLER (TOP 10)

CROSS-BORDER COMPLAINTS WITH DPC AS CONCERNED SUPERVISORY AUTHORITY (CSA)

In the period May 2018 to September 2022, 187 cross-border complaints were lodged with the DPC where another EU/EEA supervisory authority was the lead supervisory authority. The organisations against which complaints were made included KLM, Amazon, eBay, Lufthansa, Uber, Netflix, Mastercard, TAP Air Portugal, FedEX, Air France, PayPal, Brittany Ferries and Spotify.

Given the proximity of the UK to Ireland, and the multiple businesses that offer services to UK and Irish individuals, a large proportion of CSA complaints handled by the DPC involved the UK Information Commissioner's Office (ICO) as the lead supervisory authority, which were therefore heavily impacted by Brexit. Removing UK cases from the statistics shows that **48%** of the complaints sent by the DPC to other EU/EEA LSAs have been concluded.

DPC AS CSA	NUMBER OF COMPLAINTS CONCLUDED (UK INCLUDED)	NUMBER OF COMPLAINTS CONCLUDED (UK EXCLUDED)
CONCLUDED as at 19/9/2022	140 (75%)	40 (48%)

Figure 7. TOTAL CROSS-BORDER COMPLAINTS CONCLUDED WHERE DPC IS CSA

Excluding complaints where the UK was the LSA, at 19 September 2022, **10 (25%) complaints were concluded outside of the GDPR Article 60 process**. In some of these cases, the LSA sent the DPC the response of the Data Controller or summarised it in a letter to the complainant and asked the DPC to offer the controller's response to the complainant as a resolution for their complaint. In other cases, the LSA sent the DPC a letter to send to the complainant which informed them that the LSA considered it was not in a position to further investigate the complaint.

14 (35%) concluded complaints where the DPC was CSA were concluded by way of a GDPR Article 60 decision. Of these, the complaint was upheld in nine cases, rejected in one case and dismissed in four cases.

The remaining **16 (40%) of complaints were withdrawn by the complainants**.

APPENDIX 1 – AMICABLE RESOLUTION CASE STUDIES

Below is a sample of cross-border complaint cases that were resolved by means of the amicable resolution process. Sections 108 and 109 of the Data Protection Act, 2018 place an obligation on the DPC to handle complaints in accordance with Part 6 of that Act.

An important component of the complaint handling process is the obligation placed on the DPC to consider, in the case of every complaint received, whether there is a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint and, if so, to take such steps as the DPC considers appropriate to arrange or facilitate such an amicable resolution.

The DPC has long experience in the arranging or facilitation of the amicable resolution of data protection complaints as amicable resolution has been provided for in Irish data protection law since 2003. From that experience, the DPC is aware that for many complainants, their desire in submitting a data protection complaint is to have the issue resolved to their satisfaction, whether it be in relation to non-compliance with a subject access, non-compliance with an erasure request, or another data protection matter. Once the data controller fulfils those obligations in the context of the DPC's complaint handling process, the complainant is often satisfied to consider the matter concluded on the basis that an amicable resolution has been reached. However, there are other complaint cases where amicable resolution is not achievable or not an appropriate course of action and, in those cases, the preparation by the DPC of a draft decision for submission to the concerned supervisory authorities has a key role to play. This may occur in instances where amicable resolution has been attempted but agreement could not be reached between the parties within a reasonable time to resolve the complaint. It could also occur in a situation where the DPC, on assessing the complaint, considered that there is no reasonable likelihood of the parties concerned reaching an amicable resolution within a reasonable time.

As the case studies below demonstrate, the pursuit of the amicable resolution by the DPC of complaints can lead to their successful resolution in a manner that fully satisfies complainants who, in many cases, simply want a resolution of the data protection issues of concern that have arisen in their engagement with data controllers. Amicable resolution, which has a statutory basis in the Data Protection Act 2018, has proven to be a successful mechanism for the achievement of a desired outcome for many complaints handled by the DPC and the DPC continues to invest significant time and effort in exploring all options that may lead to amicable resolutions that satisfy the parties to complaints.

Meta Platforms Ireland Limited

The DPC received a complaint in March 2020 from the Austrian Data Protection Authority on behalf of an Austrian resident complainant against Meta Platforms Ireland Limited ("Facebook"). The complaint concerned a request for the erasure of personal data, as per Article 17(1) GDPR that the complainant had made to Facebook concerning his Instagram account.

The complainant in the matter had lost access to his Instagram account and was thus unable to use the in-account deletion tool provided on the platform. He had therefore made a number of requests to Facebook for the erasure of his personal data. Following his requests, he asserted that he was not provided with the necessary assistance and that his request was not actioned. The desired resolution of the complainant was to obtain the erasure of his Instagram account, and all associated personal data.

This complaint was identified as potentially being capable of amicable resolution under Section 109 of the Data Protection Act 2018. The DPC engaged in correspondence with Facebook and the complainant in an attempt to address the issues identified in the complaint and reach a satisfactory conclusion. In correspondence to the DPC, Facebook noted that the account of the complainant was currently enrolled in a checkpoint. A checkpoint is a system that prevents users from accessing their accounts until they complete some set of required steps or actions.

In working towards a resolution of the matter, Facebook offered that its specialist team would contact the complainant in order to assist him in verifying his ownership of the account and regaining access. The complainant would be required to provide a new email address that could be associated with the account. Once Facebook could confirm that the complainant was the rightful owner of the account, he would be able to access the account, use the in-app deletion tool and obtain his desired resolution.

The DPC thereafter contacted the complainant to explain the proposed amicable resolution and the complainant confirmed that he wished to proceed in this manner. The complainant provided a new email address to be associated with the account and the DPC communicated this to Facebook. The DPC further instructed Facebook to contact the complainant and assist him in obtaining the erasure of his personal data.

Facebook thereafter confirmed that its specialist team had engaged with the complainant and the complainant ultimately confirmed to the DPC that he was successful in accessing his account and obtaining its erasure. He noted his satisfaction with this outcome and he confirmed the complaint was amicably resolved. As a result,

the DPC considered the complaint amicably resolved and withdrawn, pursuant to section 109(3) of the Data Protection Act 2018.

Airbnb Ireland

The DPC received a complaint in September 2020 relating to a request for access (under Article 15 of the GDPR), that the complainant had made to Airbnb Ireland UC ("Airbnb"). The complaint was made directly to the DPC, from a data subject based in Malta. Upon assessment by the DPC, the complaint was deemed to be a cross-border one because it related to Airbnb's general operational policies and, as Airbnb is available throughout the EU, the processing complained of was therefore deemed to be of a kind "....which substantially affects or is likely to substantially affect data subjects in more than one Member State" (as per the definition of cross-border processing under Article 4(23) of the GDPR).

The complainant submitted an access request to Airbnb. Airbnb facilitated this access request by providing the complainant with a link to an access file containing his personal data. However, when the complainant tried to use the link, it was not operational. In addition, the complainant was frustrated with the difficulty they faced in contacting Airbnb in relation to this matter. The complainant submitted their complaint to the DPC on this basis.

This complaint was identified as potentially being capable of amicable resolution under Section 109 of the Data Protection Act 2018. The DPC contacted Airbnb and asked that it facilitate the complainant's request. The DPC specified that Airbnb should ensure any links it sends to complainants are fully tested and operational. In reply, Airbnb explained that once it was informed that the initial link it sent to the complainant was not operational, it sent a renewed link to the complainant and was unaware that the complainant had had any difficulty in accessing this second link. Nonetheless, in the interests of amicably resolving the complaint, Airbnb agreed to provide an additional link to an access file to the complainant and for an encrypted file to be sent to the complainant via secure email.

As a result, the matter was amicably resolved pursuant to section 109(3) of the Data Protection Act 2018 ("the Act"), and under section 109(3) of the Act the complaint was deemed to have been withdrawn. This case study demonstrates the benefits — to individual complainants — of the DPC's intervention by way of the amicable resolution process.

In this case, the DPC's involvement led to the complainant being able to access his data. This case study illustrates how often simple matters such as links which do not operate properly can become data protection complaints if the matter is not managed appropriately at the front end of data controllers' customer service and data protection teams.

Google (YouTube)

The DPC received a complaint in September 2020, via its complaint webform, against Google Ireland Limited ("**YouTube**"). The complaint was made by a parent acting on behalf of their child and concerned a YouTube channel/account. The YouTube channel/account had been set up when the child was 10 years old and at a time when they did not appreciate the consequences of posting videos online.

Although the complaint was made directly to the DPC, from an Irish resident, upon assessment it was deemed to constitute a cross-border complaint because it related to YouTube's general operational policies and, as YouTube is available throughout the EU, the processing complained of was therefore deemed to be of a kind "which substantially affects or is likely to substantially affect data subjects in more than one Member State" (as per the definition of cross-border processing under Article 4(23) of the GDPR).

According to the complaint, the child no longer had control over the account as they had lost their passwords and the account was no longer in use. However, classmates of the child had discovered the videos, which were now the subject of embarrassment to the child. The parent of the child had engaged in extensive correspondence with Google, seeking inter alia the erasure of the account from the YouTube platform. The parent had provided the URL for a specific video on the account and for the account itself. The parent was informed by Google, on a number of occasions that it had taken action and removed the content from the platform. However, the parent repeatedly followed up to note that the content had not in fact been removed and was still available online. As she considered that the complaint had not been appropriately addressed she thus raised the matter with the DPC.

This complaint was identified as potentially being capable of amicable resolution under Section 109 of the Data Protection Act 2018, with both the data subject and data controller agreeing to engage with the DPC to try to amicably resolve the matter. The DPC investigated the background to the complaint and noted that it appeared that Google had removed a specific video from the account, for which the URL had been provided, but not removed the account in its entirety, with the result that further videos remained online.

The DPC communicated with Google on the matter and informed Google of the particular background of the complaint. Google immediately took action and removed the YouTube account in its entirety. Google confirmed that a misunderstanding had arose as its support team had incorrectly assessed the URL for a specific video provided by the complainant, rather than the entire account.

The DPC informed the parent of the outcome and proposed an amicable resolution to the complaint. The parent thereafter informed the DPC that she had recently become aware of another YouTube channel which her child had created, which again was no longer in use, and which the child wanted deleted. The DPC thus corresponded further with Google and Google confirmed it had taken immediate action to remove the account and informed the parent of the actions they had taken.

This case highlights that the DPC can assist data subjects during the amicable resolution process in explaining their particular requests to a data controller, often at the appropriate level, when a data subject has previously been unsuccessful in initial engagement with the data controller. This further allows the DPC to monitor the compliance of data controllers by taking note of any issues that may repeat across complaints.

Yahoo EMEA Limited

The DPC received a complaint in March 2021 from the Bavarian data protection authority on behalf of a Bavarian complainant against Yahoo EMEA Limited.

The complainant in this matter had lost access to his AOL email account following an update on his computer. The complainant noted that he had engaged with Yahoo in order to regain access and was asked for information related to the account, which he asserted that he had provided. Yahoo informed the complainant that it could not verify his identity with the use of the information that had been provided, but it was unclear to the complainant which information was considered inaccurate. The complainant thus made a complaint to his local supervisory authority, who referred the complaint on to the DPC in its role as Lead Supervisory Authority for Yahoo.

This complaint was identified as potentially being capable of amicable resolution under Section 109 of the Data Protection Act 2018, with both the data subject and data controller agreeing to engage with the DPC to try to amicably resolve the matter.

The DPC contacted Yahoo on the matter, and Yahoo took a proactive approach and immediately noted its desire to reach out to the complainant directly to seek to resolve

the issue as soon as possible. Yahoo thereafter quickly confirmed to the DPC that its member services team made contact with the complainant, who provided alternative information that enabled Yahoo to successfully validate them and subsequently restore their account access.

This case highlights that further direct engagement between the parties during the amicable resolution process can achieve a swift resolution for data subjects. It further highlights that a proactive approach on the part of data controllers in the early stages of a complaint can often resolve matters and avoid the need to engage in a lengthy complaint handling process.

Ryanair

An individual made an access request in January 2020 to Ryanair for customer data held in relation to a flight booking. The individual did not receive a response from Ryanair and subsequently submitted a complaint to the DPC in April 2020. In June 2020, having assessed the complaint and considered itself competent to act, the DPC outlined the complaint to Ryanair. This complaint was identified as potentially being capable of amicable resolution under Section 109 of the Data Protection Act 2018. The DPC requested Ryanair review the complaint and contact the individual directly to provide them with their requested data.

In November 2020, following additional follow up by the DPC with Ryanair, the complainant informed the DPC that Ryanair had contacted them explaining that it would provide them with their requested data and would look into a separate customer service related request associated with the booking which fell outside the scope of the data protection related complaint with the DPC.

Separately, Ryanair provided the DPC with a copy of a letter sent to the complainant. Ryanair stated that its customer services department had mistakenly overlooked the complainant's access request when dealing with the customer services complaint which was the reason the access request had not been responded to. Ryanair informed the DPC that it had provided additional training to customer services staff, reemphasising the importance of recognising access requests when contained in customer services complaints.

Ryanair enclosed with this letter a copy of the requested flight booking including payment, contact and passenger details, and a copy of chat transcripts regarding the booking, as requested by the complainant. Ryanair apologised for the delay in responding to the complainant's request. The complainant confirmed to the DPC that it

was satisfied with the actions taken by the DPC to amicably resolve the complaint and thanked the DPC for its time and effort.

This case illustrates how effective and efficient amicable resolution can be for complainants and data controllers. From initial submission to conclusion, which was in the midst of the Covid-19 pandemic, the complaint took 8 months to handle and bring to an acceptable conclusion for all parties concerned. The complainant in this case received their requested data in addition to a resolution for their separate customer service related issue. The data controller was alerted to the fact that members of the customer service team needed refresher training regarding data protection requests, which formed part of customer service complaints and it delivered that training to avoid similar issues arising in the future.

Meta Platforms Ireland Ltd.

The DPC received a complaint in June 2021, directly from a complainant, against Meta Platforms Ireland Limited ("Facebook").

In their complaint, the data subject raised concerns in relation to an erasure request made to Facebook under Article 17 of the GPDR. The complainant sought to have their personal data, contained in a Facebook profile, originally set up by the complainant, but which they no longer used or had access to, deleted. The complainant asserted that their initial attempts to resolve the matter directly with Facebook had not resulted in a satisfactory conclusion and despite the complainant's requests the personal data in question had not been deleted.

This complaint was identified as potentially being capable of amicable resolution under Section 109 of the Data Protection Act 2018. The DPC informed Facebook of the complaint, outlining the substance of the complaint and seeking replies from Facebook, as part of the complaint handling process. The DPC further informed Facebook of its obligations as a data controller in relation to an erasure request.

The data subject subsequently informed the DPC that Facebook had agreed to delete the account in question. The data subject noted that this resolved their complaint to the DPC and they thanked the DPC for assisting in obtaining the erasure of their data. As a result of the confirmation received from the data subject, the complaint was considered amicably resolved and withdrawn, pursuant to section 109(3) of the Data Protection Act 2018. Facebook and the data subject were informed of the outcome.

Twitter International

The DPC received a complaint in April 2021 from the Swedish Data Protection Authority on behalf of a Swedish resident complainant against Twitter International Company ("Twitter").

In their complaint, the data subject raised concerns in relation to an erasure request made to Twitter under Article 17 of GPDR. In this regard, the data subject noted that their old Twitter account had been hacked and they no longer had access to it. However, their image and full name appeared on the account and they wished to have it erased. The data subject noted that they had contacted Twitter and failed to obtain the erasure of the account. The data subject further referred to Twitter's policy on inactive accounts and considered that their account should have been deactivated in line with this policy.

This complaint was identified as potentially being capable of amicable resolution under Section 109 of the Data Protection Act 2018. As part of its complaint handling process, the DPC engaged in correspondence with Twitter and the data subject in an attempt to address the issues identified in the complaint and reach a satisfactory conclusion for the data subject. In response to the DPC, Twitter confirmed that the account in question had been inactive for a substantial period. As a result of this, Twitter confirmed that the account would be deactivated without the requirement for any further steps on the part of the data subject.

The DPC in turn corresponded with the data subject, via the Swedish SA, to seek confirmation that this had amicably resolved their complaint. The data subject confirmed that their desired resolution to the complaint had been achieved and thanked the DPC for its efforts in resolving the issue. As a result, the DPC considered the complaint amicably resolved and withdrawn, pursuant to section 109(3) of the Data Protection Act 2018.