CEDPO

CONFEDERATION OF EUROPEAN
DATA PROTECTION ORGANISATIONS

Right Of Access
A CEDPO Comparative Analysis

Key questions of DPOs and Data Controllers

Table of contents

Countries / Right of Access	GDPR	AUSTRIA	FRANCE
Legal sources/texts	Regulation 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data: article 15 “Right of access for the data subject”, article 12 “Transparent information, communication and modalities for the exercise of the rights of the data subject”, article 23 (“Restrictions”) and article 89 (“Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes”); recitals 59, 63, 64 & 73.	Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000): Article 1, §§ 26, 50e, 52 Abs. 2a There are additional rules concerning the right of access. E.g.: Criminal Records Act 1968 (Strafregistergesetz 1968). The answers to the questionnaire only refer to the Federal Act concerning the Protection of Personal Data.	Data Protection Act of January 6, 1978 : Articles 31, 32, 38, 39 and 40 Implementation Decree n° 2005-1309 of 20 October 2005 : Articles 48, 86, 90, 92-98 Public Health Code : Articles L-1111-5 and L-1111-7 Article R 625-11 of the Criminal Code
Resources	http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf Awaiting documentation by Working Party 29, BEREC and others.	Übersicht Auskunftsrecht nach dem Datenschutzgesetz (http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=25302iob)	Guide published by the CNIL, French DPA
Before the reply			
Are we bound to respond to the request by an individual to access personal data relating to him?	Yes, knowing whether personal data is being processed is a right for the data subject. If the controller does not intend to give this information, it should explain why. Where this information is not revealed, the data subject could file	Yes, even if the data subject doesn´t provide the preliminary verifications. At least the data controller has to give the requesting person a reason why information is not or not completely provided.	Yes, unless we can claim one of the limits (see below). The so-called “access right” is one of the key rights of the Data Protection Act. Failure to comply triggers a penal fine of the 5th class (article R 625-11 of the criminal code): up to €1.500 to be

Countries / Right of Access	GDPR	AUSTRIA	FRANCE
	a complaint to the Supervisory Authority. This authority is entitled to issue fines "effective, proportionate and dissuasive" (art. 83.1). Administrative fines may go up to 20 000 000 EUR, or in case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher (art. 83.5b).	The Data Protection Authority (Datenschutzbehörde) decides on complaints of persons or group of persons who allege to have been infringed in their right of access. Failure to comply can cause an administrative offence, which is punished with a fine up to € 500.	multiplied by 5 for a legal entity. The CNIL can also order sanctions including a warning, possibly public, or an administrative fine up to €150.000. The highest sanction ordered by the CNIL so far was a public fine of €10.000 in 2012.
Is there a legal timeframe to respond?	The controller should be obliged to respond to requests of the data subject without undue delay and at the latest within one month. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests.	The data controller´s answer has to be provided within 8 weeks of the receipt of the request.	Within two months from the receipt of the request. A special regime applies to Healthcare data: the legal timeframe to reply is from 2 to 8 days and 2 months if the data goes back more than five years.
Who is bound to respond?	The data controller has to respond. He/She/It is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (art. 4.1).	The data controller has to respond (§ 26).	The data controller. More precisely it will be the department where the access right can be exercised. It is indeed required to identify such a department in the data protection notice (art. 90 Implementation Decree).
Any preliminary verifications?	The controller should use all reasonable measures to verify the identity of a data subject who requests access. As a general rule, a controller should not retain, acquire or process additional information for the sole purpose of being able	The data subject has to prove his/her identity in an "appropriate manner". The Data Protection Authority suggests providing a signed request and an ID, so that the data controller can verify the signatures. The request for information can be made orally (if the data controller	The individual has to provide an ID. If the request is in writing, the ID and the signature must be verified as well as the indication of a response address.

Countries / Right of Access	GDPR	AUSTRIA	FRANCE
	to comply with the GDPR. However, where the controller is able to demonstrate that it is not in a position to identify the data subject, it shall inform the data subject accordingly, if possible. In such case, the access right shall not apply except where the data subject, for the purpose of exercising this right provides additional information enabling his/her identification (Article 11).	agrees) or in written form.	
Can we ask the individual to precise his/her request?	Yes, but only if the controller processes a large quantity of information concerning the data subject.	Yes we can ask the individual to precise his/her request. Upon inquiry, the person requesting information has to cooperate in the information procedure to a reasonable extent to prevent an unwarranted and disproportionate effort on the part of the data controller.	We cannot ask the individual to justify his/her request. He/she has a right to curiosity. However, if the request is vague or does not contain all the items allowing to carry out the operations required, we can invite the applicant (by a letter delivered against signature or an electronic communication) to bring them before the expiry of the response period. The request for further information shall suspend the response timeframe.
What if the request is not made by the concerned individual?		Instead of the concerned individual, the request can be made by a legal representative or by any other person who is able to prove that he/she is authorised to exercise the access right for the concerned individual.	We can respond only if the person represents the concerned individual, e.g. parents for minor (exception under art. L 1111-5 of Healthcare Code) or person holding a written mandate specifying its purpose, the names of the applicant and representative, and including a copy of their IDs.

Countries / Right of Access	GDPR	AUSTRIA	FRANCE
Shall we respond to the concerned individual directly?	Yes	We have to respond to the concerned individual directly or to his/her representative.	In most instances, the response must be sent to the individual or his/her representative (see above). There are instances where the access right is a so-called “indirect access right”. It shall be exercised with the CNIL, not with the data controller (Articles 41 and 42 of the Data Protection Act). Impacted data controllers must refer the concerned individuals to the CNIL. This rule applies to processing involving State security, defence or public safety. Other large public files such as FICOBA (bank accounts) are also in the scope. Regarding health data, the patient can decide to access it directly or through a physician that he/she designates to this purpose (Art 43 Data Protection Act).
The reply			
Content of the response?	The reply must contain: 1. the purposes of the processing; 2. the categories of personal data concerned; 3. the recipients or categories of recipients to whom the personal data have been or will be disclosed	The information has to contain: 1. the processed data, 2. the information about their origin, 3. the recipients or categories of recipients of transmissions	The right of access covers any and all personal data processed by the data controller, unless it is possible to claim a limit (see below). An individual has the right to obtain: 1° confirmation as to whether the personal data relating to him form part of the processing;

Countries / Right of Access	GDPR	AUSTRIA	FRANCE
	4. if possible, the envisaged period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period 5. the existence of the right to request from the controller rectification or erasure of personal data, and of restriction or objection to the processing 6. the right to lodge a complaint to a supervisory authority 7. where the personal data are not collected from the data subject, any available information as to their source 8. In case of profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. In addition, if personal data are transferred to a third country or to an international organisation, the data subject shall have the right to	4. the purpose of the use of data 5. the legal basis of the use of data. If the data subject demands, the names and addresses of processors have to be disclosed, in case they are charged with processing data relating to him. If no data of the person requesting information exist, it is sufficient to disclose this fact.	2° information relating to the purposes of the processing, the categories of processed personal data and the recipients or categories of recipients to whom the data are disclosed; 3° if applicable, information relating to the transfers of personal data intended towards a State that is not a Member State of the European Union; 4° communication, in an accessible form, of the personal data relating to him as well as any available information on the origin of the data; 5° information allowing him to know and to object to the logic involved in the automatic processing, in case of a decision taken on the basis of automatic processing and producing legal effects towards him.

Countries / Right of Access	GDPR	AUSTRIA	FRANCE
	be informed of the appropriate safeguards (see art. 46).		
Must we provide: video and sound recordings, credit scores, codes, information in free text fields?		If the request concerns video surveillance, the data controller has to send a copy of the processed data in a common technical format to the requesting person. Sound recordings must be provided, as well as credit scores and codes. Everybody has the right of access concerning automated personal data as well as manual personal data (e.g. filing systems). As a consequence, information in free text fields has to be given to the requesting person.	Video and sound recording: Yes, the access right applies to any media. Credit scores, codes: Yes. Note that if the information is not intelligible as such, the data controller must provide a lexicon explaining codes, abbreviations and initials. Information in free text fields : Indeed
Data Format	The controller shall provide a copy of the personal data undergoing processing. Unless otherwise requested by the data subject, when the data subject makes the request by electronic means, the data must be provided in an electronic form which is commonly used.	The information should be provided in “intelligible form”. It has to be understandable.	The data should be transmitted ‘in an accessible form’. It must be clear and understandable.
Any security measures required?	Recital 63: Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his/her personal data.	The data controller has to ensure that data security is taken by all organisational units. He/she is liable for it. It is not obliged to use registered letters.	In case of doubt as to the address provided or the identity of the applicant, the response can be sent by registered letter with return receipt requested.

Countries / Right of Access	GDPR	AUSTRIA	FRANCE
What if the access request is made on the spot/ on site?		With the consent of the person requesting information, the information may be provided orally alongside with the possibility to inspect and make duplicates or photocopies instead of being provided in writing. In other words: With the data subjects' agreement it is possible to just show him or her the screen of a computer.	Access can be provided by showing either computer screens of paper copies. The protection of the personal data of third parties must be ensured. The applicant can obtain immediately a copy of the personal data unless it is contrary to a legislative or regulatory provision.
Limits - Conditions			
Can we exclude some data from the reply?	The right to obtain a copy of the personal data undergoing processing shall not adversely affect the rights and freedoms of others. Some examples are given (see recital 63) such as the protection of trade secret or the protection of intellectual property (however, the result of these exceptions should not be that all information is refused to the data subject). Member States can also pass laws limiting the right to access in order to protect, among others, rights and freedoms of the data subject and others, to protect important economic or financial interest of the Union (article 23) or to protect scientific or historical research purposes, statistical purposes or	Data must be excluded if: - it is essential for the protection of the requesting person (e.g. for health reasons) - overriding legitimate interests pursued by the controller or by a third party, especially overriding public interests, are an "obstacle to furnishing the information". Data can be excluded if: - the data subject has already been given information on his/her data (Schikaneverbot)	Only in very limited instances. The access right does not enable to have access to : - personal data stored in a form that clearly excludes all risk of violating the privacy of the data subject and for a period that does not exceed that necessary for the sole purpose of creating statistics, or scientific or historical research (art 39.II of the DP Act). However these exemptions, except for processing for conservation of archives, must be mentioned in the application for authorisation or in the notification addressed to the French DPA. - Personal data relating to

Countries / Right of Access	GDPR	AUSTRIA	FRANCE
	archiving purposes on the public interest (article 89).		other individuals - Personal data which is not yet final but which is in prevision of a decision which has not yet been made (e.g. performance evaluation process). Once the decision is made, all data kept must be made available.
Can we object to some requests?	Yes, if Member State law has established a restriction applicable to the request at hand. In addition, where the controller has reasonable doubts concerning the identity of the natural person making the access request, the controller may request the provision of additional information necessary to confirm the identity of the data subject.	Data controllers may object to requests, if the requesting person does not cooperate with the data controller to prevent unwarranted and disproportionate effort on the part of the controller. E.g.: if the requesting person doesn´t provide an ID or doesn´t pay the fee Data controllers must object to requests if: - it is essential for the protection of the requesting person - overriding legitimate interests pursued by the controller or by a third party, especially overriding public interests, are an “obstacle to furnishing the information”.	Data controllers may object to requests that are obviously excessive, in particular by their number, or their repetitive and systematic character. The burden of proof is on the data controller. The French DPA gives the example of a request of an integral copy every 3 months.
Can we charge a fee?	The first copy of the information has to be given free of charge. For any further copies requested by the data subject, the controller may charge a reasonable fee based on	The information has to be given free of charge if it concerns current data files and if the person requesting information has not yet made a request for information to the same controller regarding the same	Yes, Data controllers may require payment of a sum of money for the delivery of the copy, which shall not exceed the cost of the copy. But if it turns out that the data was

Countries / Right of Access	GDPR	AUSTRIA	FRANCE
	administrative costs where requests are manifestly unfounded or excessive.	application purpose in the current year. In all other cases a fee (€ 18,89) may be charged. If the actual costs are higher than € 18,89, the actual costs can be charged.	incorrect and has been modified as a result of the request, the individual is entitled to reimbursement.
Can we delay the answer?	The data controller has to respond to requests of the data subject without undue delay and at the latest within one month. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests.	The answer has to be provided within 8 weeks from the date the access request is received. There is no obligation to respond "as soon as possible".	In case the access request is made on site and the requested data is not readily available to be shown, then access can be delayed. Then the individual must be given a dated and signed receipt acknowledging his/her request.
Contact	international@afcdp.net	info@argedaten.at	international@afcdp.net
Authors	Pascale Gelly, Grégoire Delette – AFCDP	Philipp Hochstöger	Pascale Gelly, Bruno Rasle, Corentin Hellendorff - AFCDP

Countries / Right of Access	GERMANY	IRELAND	POLAND	SPAIN
Legal sources/texts	*Public bodies of the Federation or private bodies:* Federal Data Protection Act in the version published on January 14, 2003, last amended by Art. 1 G of the Order of February 25, 2015: Sect. 34 for *Public bodies of the "Länder":* Respective section of the State Data Protection Act ("Landesdatenschutzgesetz") Additionally, there are sectorial rules for data controllers in the field of social security, public health etc. The following analysis only refers to the Federal Data Protection Act as it affects all private bodies.	Section 4 of the Data Protection Acts 1988 & 2003 Data Protection (Access Modification) (Health) Regulations, 1989	Chapter 4 (the Rights of the Data Subject) of the Act of August 29, 1997 on the Protection of Personal Data	Basic Law 15/1999, of 13 December, on protection of personal data: Article 4(6), 5, 15, 17, 18, 20, 23 https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750 Royal Decree 1720/2007, of 21 December, developing Basic Law 15/1999, of 13 December, on protection of personal data: Articles 23 to 30 http://www.boe.es/buscar/doc.php?id=BOE-A-2008-979 DPA Instruction 1/2006, on video-surveillance: Article 5 https://www.boe.es/buscar/doc.php?id=BOE-A-2006-21648
Resources	Guide published by the Federal Commissioner for Data Protection and Freedom of Information (BfDI)	Guide for data subjects published by Data Protection Commissioner (Irish DPA) Guidance for Data Controllers on Access Requests for Personnel Records Case Studies on right of access published by Data	n/a	Spanish DPA guidelines: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO_OK.pdf Specific section of the Spanish DPA website: http://www.agpd.es/portalw

Countries / Right of Access	GERMANY	IRELAND	POLAND	SPAIN
		Protection Commissioner		ebAGPD/CanalDelCiudadano/derechos/index-ides-idphp.php
	Before the reply			
Are we bound to respond to the request by an individual to access personal data relating to him?	Yes, unless the exemption clause of Sect. 34 para. 7 (referring to Sect. 33 para. 2 no. 1, 2, 3 5-7) applies. Failure to comply can result in an administrative offences punishable by a fine up to €50.000 (Sect. 43 no. 8a Federal Data Protection Act). The fine shall exceed the financial benefit to the perpetrator derived from the administrative offence. If the amount of €50.000 is not sufficient to do so, the fine may be increased.	Yes. There is no direct fine or penalty for failure to comply, but a data subject has the right to complain to the Data Protection Commissioner, who must investigate and give a decision. If the Commissioner issues an Enforcement Notice requiring the data controller to respond, failure to comply with the notice is a criminal offence. Separately, if data subjects can show they suffered harm or loss as a result of the data controller's failure to respond, they could in principle sue for damages.	Yes. There is no direct fine or penalty for failure to comply with a data subject request. However, data subject has the right to complain to the Inspector General for Personal Data Protection. If the Commissioner issues an Enforcement Notice requiring the data controller to respond, failure to comply with the notice may result in administrative fines up to approx. € 12,000 (or up to € 48,000 in case of multiple breaches). Also, if data subjects can show they suffered harm or loss as a result of the data controller's failure to respond, they could in principle sue for damages.	Yes. Even if the request cannot be accepted (see below), the data controller must nevertheless inform the applicant of that circumstance within the prescribed time period. The so-called "access right" is one of the key rights of the Data Protection Act. Failure to comply triggers an administrative fine up to Euro 300,000.
Is there a legal timeframe to respond?	The Federal Data Protection Act does not stipulate a timeframe for responding to access requests. In general the data controller's answer	Yes. The data must be supplied "as soon as may be and in any event not more than 40 days" after a valid request is received.	Yes. The data must be supplied within 30 days upon receiving a valid request.	The data controller must reply to the request for access within 30 days of its receipt and provide effective access within 10 days of

Countries / Right of Access	GERMANY	IRELAND	POLAND	SPAIN
	has to be provided within a reasonable period of time. The Data Protection Authority of Lower Saxony considers 3 weeks to be an appropriate timeframe to respond (Link).	In other words, 40 days is a maximum and a controller cannot decide, for example, as a matter of policy always to wait 40 days before providing the data.		issuing its reply.
Who is bound to respond?	The data controller has to provide the information (Sect. 34 para. 1, sentence 1 Federal Data Protection Act).	The data controller.	The data controller.	The data controller must always respond. The data processor may answer the request if it has been specifically entrusted to do so by the data controller in the data processing agreement (the answer is therefore made on behalf of the data controller). If the data subject does not receive a proper or timely answer, it may lodge a claim before the DPA, which shall initiate specific proceedings ("*tutela de derechos*") aimed at obtaining the adequate response from the controller. If the controller does not comply with the DPA order, a fine may be imposed.
Any preliminary verifications?	Sect. 34 of the Federal Data Protection Act does not oblige data controllers to	The data subject must provide the controller with such information as the data	The data subject has to make sure to provide enough information that the data	The individual must provide a photocopy of his/her national identity document,

Countries / Right of Access	GERMANY 	IRELAND 	POLAND 	SPAIN 
	perform preliminary verification methods. The Federal Commissioner for Data Protection and Freedom of Information (BfDI) recommends that data controllers should accept access requests only in writing in order to make sure that the data subject and the addressee are identical (Link).	controller "may reasonably require in order to satisfy himself of the identity of the individual and to locate any relevant personal data or information." The request must be in writing and accompanied by the fee, if it is charged by the data controller. Currently, the maximum fee is €6.35.	controller can be reasonably sure that the request comes from the data subject.	or his/her passport or other valid identifying document and, if necessary, of the person representing him/her, or equivalent electronic instruments. If the access right refers to a video-surveillance recording, an updated picture shall also be required.
Can we ask the individual to precise his/her request?	The data subject should provide a detailed description of the type of personal data he/she would like information about (Sect. 34 para. 1, sentence 2 Federal Data Protection Act). According to the Federal Commissioner for Data Protection and Freedom of Information (BfDI) a request seeking for information as regards • the stored data about the data subject, • the origin of such data, • the recipient or type of recipients to whom the data are	Data subjects cannot be required to explain the reasons for their request. They may be required to provide such information as the data controller "may reasonably require in order to . . . locate any relevant personal data or information."	Data subjects do not need to explain the reasons for their request. Also, there is a general assumption that data subject requests apply to all types of data held by the data controller, unless request specifies otherwise.	We cannot ask the individual to justify his/her request.

Countries / Right of Access	GERMANY 	IRELAND 	POLAND 	SPAIN 
	provided and • the purpose of data processing is considered to be precise (Link).			
What if the request is not made by the concerned individual?	A declaration of intent which a person makes within the scope of his/her own power of agency in the name of a principal takes effect directly in favour of and against the principal (Sect. 164 Civil Code). Consent (granted by the principal) shall be given in writing unless special circumstances warrant any other form (Sect. 4a, sentence 3 Federal Data Protection Act).	The request must be made by the data subjects, but can be made on their behalf, for example by a legal representative, parent, or guardian. In these cases, given the data controller's duty to keep data safe & secure from unauthorised disclosure, the controller would need to be satisfied that the person submitting the request had the data subject's permission to do so.	The request can be made either by the data subjects him/herself or by a legal representative (attorney, parent, or guardian). Any such third party has to provide valid proof of authorisation to act on behalf of data subject.	The access right may be exercised: • By the data subject; • By the data subject's legal representative (e.g., minor), who must evidence his/her legal status; or By a voluntary representative of the data subject, expressly designated for the exercise of the access right.
Shall we respond to the concerned individual directly?	The response must be sent to the individual or his/her representative.	The data must be provided to the data subjects or their representatives.	The data must be provided to the data subjects or their representatives, depending on the request.	In all cases, the response must be sent to the individual or his/her authorised representative (see above).
	The reply			

Countries / Right of Access	GERMANY 	IRELAND 	POLAND 	SPAIN 
Content of the response?	Sect. 34 Federal Data Protection Act: (1) At the request of the data subject, the controller shall provide information 1. on stored data about the data subject, also where they refer to the origin of these data, 2. on the recipient or type of recipients to whom the data are provided, and 3. the purpose of processing. There are additional requirements such as in the event of transferring personal data for direct marketing purposes of third parties (Sect. 34 para. 1a Federal Data Protection Act), Scoring (Sect. 34 para. 2 Federal Data Protection Act), the commercial collection and storage of data for the purpose of transfer (Sect. 34 para. 3 and 4	(1) A copy of the data subject's personal data (if any) in permanent and intelligible form. (2)A description of the categories of data being processed. (3) Details of the source of the data. (4) A description of the purpose(s) for which the data is being processed. (5) Details of who the data may be disclosed to. (6) Where decisions may be made concerning the data subject by entirely automated means, an explanation of the logic involved in the decision making process.	Data subject has the right to obtain information: 1) on whether such system exists and to establish the controller's identity, the address of its seat and its full name, and in case the controller is a natural person to obtain his/her address and his/her full name ; 2) as to the purpose, scope, and the means of processing of the data contained in the system ; 3) since when his/her personal data are being processed; 4) as to the source of his/her personal data, unless the controller is obliged to keep it confidential as a state, trade or professional secrecy ; or 5) about the means in which the data are disclosed, and in particular about the recipients or categories of recipients of the data.	The data subject is entitled to request and obtain information from the data controller regarding: • the personal data that is being processed (including data initially collected or resulting from any further data processing operation, as the case may be); • the precise uses and purposes of the data processing; • the origin of the personal data (each source should be specified if the data is collected from multiple sources); and the disclosures or transfers carried out or which are expected to be carried out in respect of the same (indicating the recipients to whom the data is disclosed or to be disclosed).

Countries / Right of Access	GERMANY 	IRELAND 	POLAND 	SPAIN 
	Federal Data Protection Act) or the automated individual decision-making (Sect. 6a para. 3 Federal Data Protection Act).			
Must we provide: video and sound recordings, credit scores, codes, information in free text fields?	Yes, the access right applies to any media. Scores: Sect. 34 Data Protection Act: (2) In the cases covered by Section 28b *[Scoring]*, the decision-making body shall provide the data subject with the following information upon request: 1. probability values calculated or stored for the first time within the six months preceding the receipt of the information request, 2. the types of data used to calculate the probability values, and 3. how probability values are calculated and their significance, with reference to the individual case and in	Yes, the right of access applies to <u>all</u> automated personal data as defined in the EU directive & Data Protection Acts, and any manual (paper based) personal data which is filed in such a way as to make data about individual data subjects "readily accessible".	Yes.	Video and sound recording: Yes, the access right applies to any media. Credit scores, codes: Yes. Note that if the information is not intelligible as such, the data controller must provide a lexicon explaining codes, abbreviations and initials. Information in free text fields: Yes.

Countries / Right of Access	GERMANY	IRELAND	POLAND	SPAIN
	a form understandable to a general audience.			
Data Format	Sect. 34 Data Protection Act: (6) Upon request, the information shall be provided in written form, unless another form would be more appropriate in the circumstances.	The data subject must be provided with a "copy" of the data in "permanent form", which implies that, for example, it could not be given orally. The data must be in "intelligible" form and an explanation of any details which would not be understood by an "average" person must be provided.	The data subject may choose the format of data, provided it is "intelligible". However, data controller provide the data in paper form, if requested by the data subject.	The information must be provided in a clear, legible and recognisable manner (with no keys or codes).
Any security measures required?	Responding to an access request in writing is deemed appropriate. Using registered letters is not necessary.	The duty to keep personal data safe from unauthorised disclosure would apply.	The duty to keep personal data safe from unauthorised disclosure applies.	The application request must specify the address that must be used by the controller for notification purposes (e.g., to answer the access right). Should the data controller offer a specific system for the effective exercise of the right of access and the data subject rejects it, the data controller shall not be liable for the possible risks to the security of the information that may arise from the choice.
What if the access request is made on the spot/ on site?	Access can be provided by showing e.g. computer screens or paper copies. The protection of the personal	The data subject is still entitled to a "copy" of the data in "permanent form". So, for example, merely	Please see "Data Format" for comment.	Access may be provided on site if the data subject so requests it. Indeed, the data subject may choose to

Countries / Right of Access	GERMANY	IRELAND	POLAND	SPAIN
	data of third parties must be ensured though.	showing the data on a computer screen would not be sufficient without the data subject's agreement.		receive the information through one or several of the following file consultation systems: • Screen display. • Letter, copy or photocopy sent by post, registered or not. • Facsimile. • E-mail or other electronic communication systems. • Any other system that is suitable to the configuration or material implementation of the filing system or to the nature of the processing, offered by the data controller. if the data controller offers a specific system for the effective exercise of the right of access and the data subject demands it be done through a procedure that involves a disproportionate cost, being similarly effective and guaranteeing the same security as the procedure offered by the data controller, the costs arising

Countries / Right of Access	GERMANY	IRELAND	POLAND	SPAIN
				from such a decision shall be at the expense of the data subject.
	Limits - Conditions			
Can we exclude some data from the reply?	Only in very limited instances. Personal data relating to other individuals than the data subject has to be excluded. Furthermore, data not within the scope of the Federal Data Protection Act, such as anonymized data, can be excluded.	(1) Third party privacy rights must be respected. (2) Where the "the supply of such a copy is not possible or would involve disproportionate effort". In practice, this exemption is interpreted very narrowly. It also applies only to the supplying of the copy, not to the effort involved in locating the data in the first instance. (3) Data kept solely for the purpose of statistical research, where the statistics produced do not identify individual data subjects.	The controller has to refuse to disclose requested information, if it would lead to: 1) a disclosure of confidential information; 2) a threat to national defence or national security, to life and health of individuals or to public security and public order; 3) a threat to a vital economic or financial interest of the State; or 4) a significant breach of personal rights of the data subject or of other persons.	No, unless Spanish law specifically prohibits the data controller from replying to the access request. There are specific derogations for data controllers of the public sector (in particular, the tax authorities)
Can we object to some requests?	The exemption clause of Sect. 34 para. 7 Federal Data Protection Act allows the data controller to object to certain access requests. The excessive exercise of the access right is not mentioned within the exemption clause of Sect. 34 para. 7 Federal	«The data controller is not obliged to comply with a subsequent identical or similar request . . . by the same individual unless, in the opinion of the data controller, a reasonable interval has elapsed between compliance with the	Data controllers may object to requests that are more frequent than once every six months.	The access request must be rejected: • when the request is made by a person other than the data subject or his/her legal representative; the request is incomplete or Spanish law specifically

Countries / Right of Access	GERMANY	IRELAND	POLAND	SPAIN
	Data Protection Act.	previous request and the making of the current request. »		prohibits the data controller from replying to the access request; when the access request is made before 12 months have elapsed as from the date of a prior request by the same person that has been properly answered, unless the data subject can prove a legitimate interest.
Can we charge a fee?	Sect. 34 Data Protection Act: (8) The information shall be free of charge. If the personal data are stored commercially for the purpose of transfer, the data subject may request information in written form once per calendar year free of charge. For each additional request a fee may be charged, if the data subject can use the information for commercial purposes with respect to third parties. […]	The maximum fee currently prescribed under the Data Protection Acts is €6.35, regardless of the actual cost of responding to the request.	No.	No.
Can we delay the answer?	There are no legal provisions allowing the data controller to delay the answer. The answer has to be provided within a reasonable period of	No. The data must be provided "as soon as may be and in any event not more than 40 days" from the date a valid access request is	No, provided no extraordinary conditions take place (e.g. force majeure).	No.

Countries / Right of Access	GERMANY 	IRELAND 	POLAND 	SPAIN 
	time.	received.		
Contact	info@gdd.de	fintan@swanton.ie	info@sabi.org.pl	contacto@apep.es
Authors	Christoph Klug, Steffen Weiß	Fintan Swanton	Michal Kaczorowski	Cecilia Alvarez - APEP

About CEDPO:

CEDPO was founded in September 2011 by European Data Protection Organisations, namely, AFCDP (*Association Française des Correspondants à la Protection des Données à Caractère Personnel*) of France, APEP (*Asociación Profesional Española de Privacidad*) of Spain, GDD (*Gesellschaft für Datenschutz und Datensicherheit*) of Germany, and NGFG (*Nederlands Genootschaap van Functionarissen voor de Gegevensbescherming*) of The Netherlands. The Confederation was soon joined by ADPO (Association of Data Protection Officers) of Ireland, ARGE DATEN of Austria and SABI (*Stowarzyszenie Administratorów Bezpieczeństwa Informacji*) of Poland.

CEDPO aims to promote the role of the Data Protection Officer, to provide advice on balanced, practicable, and effective data protection and to contribute to a better harmonisation of data protection law and practices in the EU/EEA.

Contact information

Email: info@cedpo.eu / Website: www.cedpo.eu

France: AFCDP, *Association Française des Correspondants à la Protection des Données*, was created in 2004, following the modification of the Data Protection Act, which created the function of DPO ("Correspondant à la protection des données à caractère personnel" also called CIL, "Correspondant Informatique & Libertés"). AFCDP is a wide forum which welcomes any person interested in the protection of personal data: CIL, data protection managers, lawyers, HR specialists, IT and IS experts, quality and compliance managers, professionals of the e-commerce and marketing sectors … Over 1440 individuals have joined so far this non- profit association. AFCDP promotes discussion and information sharing on the protection of personal data in order to facilitate exchange among its members and to promote best practices. AFCDP maintains relationship with the French National Data Protection Commission (CNIL) and other authorities at French and European level involved in the protection of personal data.

Contact: Paul-Olivier Gibert (President), Email: president@afcdp.net; Pascale Gelly (Vice-President and International Affairs), Email: international@afcdp.net; Bruno Rasle (Délégué Général), Tel.+ 33 (0) 612340884, Email: delegue@afcdp.net

Website: www.afcdp.net

Spain: The Spanish Association of Privacy Professionals (*Asociación Profesional Española de la Privacidad*) was created in 2009 by and for different profiles related to data protection and privacy professional interests, of both the private and the public sectors: in-house lawyers and external legal counsels, IT, IS and CTI experts as well as academics. In 2010, it launches the APEP certification for accountable professionals in order to put in value the DP professional roles and thus to contribute creating trust in the dynamic and emerging privacy market. The APEP has established stable links with several DPAs as well as with privacy-related associations and institutions at the domestic, EU and international levels.

Contact: Ricard Martinez (President), Email: presidencia@apep.es; Cecilia Alvarez (Vice-President and International Affairs), Email: administracion@apep.es;

Website: www.apep.es

Austria: ARGE DATEN is Austria's leading privacy organisation. The society is committed to the protection of personal data and privacy in the age of global communication. Areas of focus are member support, public relations, information service, comments on draft laws/regulations and training. ARGE DATEN works in close cooperation with research institutions, universities, the industry and related authorities to achieve these aims. ARGE DATEN Privacy Austria was founded in 1983 as a working group and was registered as association under Austrian law in 1991. It is a non-profit making and non-governmental politically independent membership corporation. ARGE DATEN has about 700 members mostly companies and other organisations (public authorities, universities, NGOs).

Contact: Charlotte Schönherr, Email: charlotte.schoenherr@argedaten.at

Website: www.argedaten.at

dpo.ie the association of data protection officers

Ireland: The Association of Data Protection Officers (ADPO) is a membership organisation for those who are actively working as Data Protection Officers in their organisations. ADPO offers data protection officers the opportunity to share ideas, voice concerns, seek clarity on new legislation, and offer their own insights on the demands and challenges of the job. Membership is open to anyone with a data management role within their organisation, whether formally or informally. ADPO's objective is to provide clarity on issues, raise awareness of data protection legislation and to offer its members a forum where these topics can be discussed.

Contact: Fintan Swanton, Tel. +353 1 6447820, Email: info@dpo.ie

Website: www.dpo.ie

GDD

Germany: The German Association for Data Protection and Data Security (*Gesellschaft für Datenschutz und Datensicherheit – GDD*) was founded in 1977 and stands as a non-profit organisation for practicable and effective data protection. With more than 2400 – mostly company – members the GDD is Germany`s leading privacy association. Besides offering various member services such as education, training and certification of Data Protection Officers, guides for practitioners and networking opportunities for data protection professionals all across Germany, the GDD also represents member positions at national and European level.

Contact: Christoph Klug, Tel. +491704878062, Email: klug@gdd.de

Website: www.gdd.de

The Netherlands:*Het Nederlands Genootschap van Functionarissen voor de gegevensbescherming* (NGFG) is the Dutch association of Data Protection Officers, a position specified in article 62 of the Dutch Personal Data Protection Act, the Wet beschermingpersoonsgegevens (WBP). WBP has a provision where businesses, branch organisations, governments and institutions are allowed to appoint an internal supervisor for protecting the rights of data subjects, i.e. Data Protection Officers. These individuals supervise the proper implementation, as well as ensuring compliance to applicable laws, regulations and professional codes of conducts, in the field of data protection within their organization. Thanks to the statutory tasks, responsibilities and authorities, Data Protection Officers have the ability to act independently within their organizations. The appointment of Data Protection Officers is how WBP implemented the ' Data Protection Officials' as referred to in article 18, second paragraph of the Directive 95/46/EC.

Contact: Dr. Sachiko Scheuing, Email: secretariaat@ngfg.nl

Website: www.ngfg.nl

Poland: The Association of Information Security Administrators (Stowarzyszenie Administratorów Bezpieczeństwa Informacji) is a non-profit volunteer organization, which aims to strengthen the privacy professionals community. It was created in 2007 and it counts about hundred members. The activities of SABI focus mainly on integration and development of privacy professionals, who can share their experience and by building best practices. SABI strives to spread knowledge about privacy and ethical standards of privacy officers, thus it has implemented DPOs' Code of Professional Ethics.

Contact: Maciej Byczkowski, Tel. +48226201253 Email: info@sabi.org.pl

Website: www.sabi.org.pl