When ang how to respond to data subjects' requests?

Data Protection Regulation (GDPR) provides **8 fundamental rights** for individuals. Through these rights, data subjects can make a specific request as a customer, as an employee, and as personnel of a supplier.

Read more about main data subject rights and check our recommendation how to cope with the requests and respond properly.

Type of request (type of the data subject right)	What data provide and when apply?	How to provide and cope with the request?	When to provide?	Can I refuse to respond?	CORE Legal additional recommendations
Right to be informed about the collection and use of their personal data.	➢ Individuals have the right to be informed about the collection and use of their personal data. ➢ You must provide privacy information to individuals at the time you collect their personal data from them. ➢ If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month. What data you shall provide? 1. The identity and the contact details of the controller and, where applicable, of the controller's representative	Privacy notice in a accessible form (via webpage). The controller shall take appropriate measures to provide any information relating to processing to the data subject in a ➢ concise, transparent, intelligible and easily accessible form, ➢ using clear and plain language, in particular for any information addressed specifically to a child. ➢ The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.	1. You must provide privacy information to individuals at the time you collect their personal data from them. 2. If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month. 3. If you plan to communicate with the person, et the latest, when the first communication take place. 4. If you are going to disclose the data to	There are a few circumstances when you do not need to provide people with privacy information, such as if: 1. an individual already has the information or 2. if it would involve a disproportionate effort to provide it to them.	You must regularly review, and where necessary, update your privacy information. If you plan to use personal data for a new purpose, you shall Update your privacy information and communicate the changes to individuals before starting any new processing,

	2. the contact details of the data protection officer, where applicable; 3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; 4. the legitimate interests pursued by the controller or by a third party, if data processed based on legitimate interest; 5. the recipients or categories of recipients of the personal data, if any; 6. the fact that the controller intends to transfer personal data to a third country; 7. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; 8. the existence of the data subject rights 9. the existence of the right to withdraw consent at any time 10. the right to lodge a complaint with a supervisory authority 11. the existence of automated decision-making, if any.		third party, at the latest, when the data is disclosed.		
Right of access (SAR)	The individuals have the right to access and receive a copy of their personal data, and other supplementary information.	Individuals can make SARs verbally or in writing, including via social media.	Without delay and within one month of receipt of the request.	Where an exemption applies, you may refuse to provide all or some of the requested information,	Make a policy for how to record request you receive (verbally or in written).

TYPE OF REQUEST	WHAT DATA PROVIDE AND WHEN APPLY?	HOW TO PROVIDE AND COPE?	WHEN TO PROVIDE?	CAN I REFUSE TO RESPOND?	CORE LEGAL RECOMENDATION
	What information you have to provide: 1. the purposes of the processing; 2. the categories of personal data concerned; 4. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; 6. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; 7. the existence of the data subject rights 9. the right to lodge a complaint with a supervisory authority; 11. where the personal data are not collected from the data subject, any available information as to their source; 13. the existence of automated decision-making, 14. whether the personal data are transferred to a third country	If an individual makes a request electronically, you should provide the information in a commonly used electronic format, unless the individual requests otherwise. A third party can also make a SAR on behalf of another person. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. If you process a large amount of information about an individual, you may be able to ask them to specify the information or processing activities their request relates to, if it is not clear. You should perform a reasonable search for the requested information. You should provide the information in an accessible, concise and intelligible format. The information should be disclosed securely.		depending on the circumstances. The example of exemptions : crime and taxation: risk assessment, legal professional privilege (advocates); journalism, academia, art and literature You can also refuse to comply with a SAR if it is: - manifestly unfounded or - manifestly excessive. If you refuse to comply with a request, you must inform the individual of: ➢ the reasons why; ➢ their right to make a complaint to the supervisory authority; and ➢ their ability to seek to enforce this right through the courts.	Understand what steps you need to take to verify the identity of requester. You need to be satisfied that you know the identity of the requester (or the person the request is made on behalf of). If you are unsure, you can ask for information to verify an individual's identity. The timescale for responding to a SAR does not begin until you have received the requested information. However, you should request ID documents promptly. If an individual asks, you can provide a verbal response to their SAR, provided that you have confirmed their identity by other means. You should keep a record of the date they made the request, the date you responded, details of who provided the information and what information you provided. As the controller of the information you are responsible for taking all reasonable steps to ensure its security. You shall have suitable information management in

TYPE OF REQUEST	WHAT DATA PROVIDE AND WHEN APPLY?	HOW TO PROVIDE AND COPE?	WHEN TO PROVIDE?	CAN I REFUSE TO RESPOND?	CORE LEGAL RECOMENDATION
					place to allow you to locate and retrieve information efficiently.
Right to rectification	The right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. If you receive a request for rectification you should take reasonable steps to satisfy yourself that the data is accurate and to rectify the data if necessary. You should take into account the arguments and evidence provided by the data subject.	You should let the individual know if you are satisfied that the personal data is accurate, and tell them that you will not be amending the data. You should explain your decision, and inform them of their right to make a complaint to the supervisory authority	Without delay and within one month of receipt of the request.	If an exemption applies, you can refuse to comply with an objection (wholly or partly). Not all of the exemptions apply in the same way, and you should look at each exemption carefully to see how it applies to a particular request. You can also refuse to comply with a request if it is: ➢ manifestly unfounded or ➢ manifestly excessive.	Understand what steps you need to take to verify the identity of requester. You may also take into account any steps you have already taken to verify the accuracy of the data prior to the challenge by the data subject. It is a good practice to place a note on your system indicating that the individual challenges the accuracy of the data and their reasons for doing so. Determining whether personal data is inaccurate can be more complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate and should be kept. In such circumstances the fact that a mistake was made and the correct information should also be included in the individuals data.

					As a matter of good practice, you should restrict the processing of the personal data in question whilst you are verifying its accuracy, whether or not the individual has exercised their right to restriction.
Right to erasure	The right is not absolute and only applies in certain circumstances. Individuals have the right to have their personal data erased if: • the personal data is no longer necessary for the purpose which you originally collected or processed it for; • you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent; • you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing; • you are processing the personal data for direct marketing purposes	If a valid erasure request is received and no exemption applies then you will have to take steps to ensure erasure from backup systems as well as live systems. Those steps will depend on your particular circumstances, your retention schedule (particularly in the context of its backups), and the technical mechanisms that are available to you It may be that the erasure request can be instantly fulfilled in respect of live systems, but that the data will remain within the backup environment for a certain period of time until it is overwritten.	Without delay and within one month of receipt of the request.	If an exemption applies, you can refuse to comply with a request for erasure (wholly or partly). Not all of the exemptions apply in the same way, and you should look at each exemption carefully to see how it applies to a particular request. You can also refuse to comply with a request if it is: ➢ manifestly unfounded or ➢ manifestly excessive.	Understand what steps you need to take to verify the identity of requester. If you have disclosed the personal data to others, you must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individuals about these recipients.

TYPE OF REQUEST	WHAT DATA PROVIDE AND WHEN APPLY?	HOW TO PROVIDE AND COPE?	WHEN TO PROVIDE?	CAN I REFUSE TO RESPOND?	CORE LEGAL RECOMENDATION
	and the individual objects to that processing; • you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle); • you have to do it to comply with a legal obligation; or • you have processed the personal data to offer information society services to a child.				
Right to restrict processing	Individuals have the right to request the restriction or suppression of their personal data. This means that an individual can limit the way that an organisation uses their data. When processing is restricted, you are permitted to store the personal data, but not use it.	There are a number of different methods that could be used to restrict data, such as: ➢ temporarily moving the data to another processing system; ➢ making the data unavailable to users; or ➢ temporarily removing published data from a website.	Individuals have the right to request you restrict the processing of their personal data in the following circumstances: 1. the individual contests the accuracy of their personal data and you are verifying the accuracy of the data; 2. the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead; 3. you no longer need the personal data but the individual needs you to	If an exemption applies, you can refuse to comply with a request for restriction (wholly or partly). You can also refuse to comply with a request if it is: - manifestly unfounded or - manifestly excessive.	You need to have processes in place that enable you to restrict personal data if required. Understand what steps you need to take to verify the identity of requester. If you have disclosed the personal data in question to others, you must contact each recipient and inform them of the restriction of the personal data - unless this proves impossible or involves disproportionate effort.

			keep it in order to establish, exercise or defend a legal claim; or 4. the individual has objected to you processing their data and you are considering whether your legitimate grounds override those of the individual.		
Right to data portability	Information is only within the scope of the right to data portability if it is personal data of the individual that they have provided to you. The right to data portability only applies when: 1. your lawful basis for processing this information is consent **or** f 2. or the performance of a contract; and 3. you are carrying out the processing by automated means (ie excluding paper files). The right to data portability entitles an individual to: • receive a copy of their personal data; and/or	You can achieve data portability by either: ➢ directly transmitting the requested data to the individual; or ➢ providing access to an automated tool that allows the individual to extract the requested data themselves. You should provide the personal data in a format that is: ➢ structured; ➢ commonly used; and ➢ machine-readable. Where no specific format is in common use within your industry or sector, you should provide personal data using open formats such as CSV, XML and	Without delay and within one month of receipt of the request.	If an exemption applies, you can refuse to comply with a request for data portability (wholly or partly) You can also refuse to comply with a request if it is: ➢ manifestly unfounded or ➢ manifestly excessive.	You should consider the **technical feasibility** of a transmission on a request by request basis. The right to data portability does not create an obligation for you to adopt or maintain processing systems which are technically compatible with those of other organisations. However, you should take a reasonable approach, and this should not generally create a barrier to transmission. If the requested information includes information about others (eg third party data) you need to consider whether transmitting that data would adversely affect the rights and freedoms of those third parties.

	• have their personal data transmitted from one controller to another controller.	JSON. You may also find that these formats are the easiest for you to use when answering data portability requests.			
Right to object	Individuals have the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing.	Where you have received an objection to the processing of personal data and you have no grounds to refuse, you need to stop or not begin processing the data. This may mean that you need to erase personal data as the definition of processing under the GDPR is broad, and includes storing data. However, as noted above, this will not always be the most appropriate action to take.	Without delay and within one month of receipt of the request.	If an exemption applies, you can refuse to comply with an objection (wholly or partly). Not all of the exemptions apply in the same way, and you should look at each exemption carefully to see how it applies to a particular request. You can also refuse to comply with a request if it is: ➢ manifestly unfounded or ➢ manifestly excessive.	Understand what steps you need to take to verify the identity of requester. It is good practice to have a policy for recording details of the objections you receive, particularly those made by telephone or in person.
Rights related to automated decision making including profiling	GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them. The restriction only covers solely automated individual decision-making that produces legal or similarly significant effects. If your processing does not match this definition then you can continue to carry out profiling and automated decision-making.	Privacy notice in a accessible form (via webpage).	You must provide this information at the time you collect personal data and carry out this type of decision-making.		Because this type of processing is considered to be high-risk the GDPR requires you to carry out a Data Protection Impact Assessment (DPIA) to show that you have identified and assessed what those risks are and how you will address them. You must: ➢ provide meaningful information about the

TYPE OF REQUEST	WHAT DATA PROVIDE AND WHEN APPLY?	HOW TO PROVIDE AND COPE?	WHEN TO PROVIDE?	CAN I REFUSE TO RESPOND?	CORE LEGAL RECOMENDATION
	You can only carry out this type of decision-making where the decision is: ➢ necessary for the entry into or performance of a contract; or ➢ authorised by domestic law applicable to the controller; or ➢ based on the individual's explicit consent. You shall: ➢ give individuals specific information about the processing; ➢ provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual.				logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual; ➢ use appropriate mathematical or statistical procedures; ➢ ensure that individuals can: ➢ obtain human intervention; ➢ express their point of view; and ➢ obtain an explanation of the decision and challenge it; ➢ put appropriate technical and organisational measures in place, so that you can correct inaccuracies and minimise the risk of errors; ➢ secure personal data in a way that is proportionate to the risk to the interests and rights of the individual, and that prevents discriminatory effects.