Data S e Notes

SAMPLE

Introduction

The UK GDPR bestows a range ls. Individuals, or "data subjects" have the following rights, as set ou 2-23) of the UK GDPR:

- The right to be informed ab se of their personal data;
- The right of access to their
- The right to rectification of e it is inaccurate or incomplete;
- The right to have their pers
- The right to restrict or supp eir personal data;
- The right to data portability
- The right to object to the p al data (in certain circumstances); and
- Rights in relation to auton nd profiling (where this is carried out).

These Guidance Notes aim to pr of each of these rights. In some cases, more detailed guidance cuments (such as policies) are available on specific rights. Where eferenced in this document.

The Right to be Informed

You must tell data subjects abou collect. In particular, you must tell them what you collect, how you u old on to it, and whether it will be shared with anyone.

The Right of Access

If a data subject makes a *subject* st provide a copy of any personal data you hold about that individu er important information which is very similar to the information rec *informed*. Subject to some limited exceptions, you have one month t

The Right to Rectification

Data subjects have the right to /or update personal data that is inaccurate or incomplete. Subject ns, you normally have one month to comply.

The Right to Erasure

Also known as "the right to be fo ave the right to request that you erase (or otherwise dispose of) th ain cases including where it is no longer necessary for you to hold t en processed unlawfully, or if your use of it is no longer compatible w to justify that use.

The Right to Restrict Processing

Data subjects have the right to as f their personal data. This can be useful in situations where erasure such as where a data subject has contested the accuracy of their p e verifying its accuracy, or where you no longer need the person al needs you to keep it for the purposes of a legal claim. (Other c)

The Right to Data Portability

If personal data has been prov subject, is being processed by automated (i.e. electronic) means r using it is either consent or the

performance of a contract, data obtain a copy of that personal data and reuse it across different serv

The Right to Object

Where personal data is used fo ses, data subjects have the right to object to such processing. Data to processing for tasks carried out in the public interest; the exercis is vested in you; or your legitimate interests (or those of a third part lute. For example, you may be able to continue processing if you ca ng legitimate grounds that override the individual's interests, rights,

Rights Related to Automated Decisi ng

Some decisions can be made w ment. Profiling, for example, makes calculated assumptions about p l data. Data subjects have the right to challenge decisions made in human review of the processing if they believe that the rules applic are not being followed.

SAMPLE

Part 1. The Right to be Info

Transparency is one of the cor otection law. It is important that individuals know who you are, wh lect about them, what you do with it, and why. The required informat n a clear and concise manner and should be readily accessible.

When personal data is collected cts, your *privacy information* must be provided at the time personal d btain the data from a third party, it should be provided to the data sub

- Within a reasonable period ot later than one month); or
- If the personal data is us the data subject, when the first communication is made, at
- If the personal data is to b arty, when the disclosure is made, at the latest.

The Information Required

In most cases, your privacy inforr whether you collect personal data directly from individuals or from ot ference in your information will be to the extent that it relates to th e information or your source, as explained below.

You should provide the following:

- The name and contact deta
- The name and contact deta e;
- The contact details of your you have one);
- The purpose(s) for which y data;
- Your lawful basis for proce
- Your legitimate interests fo l data (if this is your lawful basis);
- The categories of person es only if collected from another source);
- The recipients or categori e sharing the personal data (you can provide specific names ate what kind of organisations you are dealing with);
- Details of any transfers third countries (i.e. non-UK) or international organisations
- How long you will keep th w you will determine how long to keep it if there isn't a fixed
- The rights available to data the processing;
- Details of the right to withd sent is the lawful basis);
- Details of the right to comp ommissioner's Office (the "ICO");
- The source of the persona ected from another source);
- Details of the statutory or quiring the data subject to provide their personal data (applies e data subject);
- Details of automated decis ofiling).

SAMPLE

Providing Your Privacy Information

Privacy information has various s the same thing. Privacy policy, privacy statement, and privacy ms. Some might also use “data protection policy”, although this is n internal policy of much broader scope (as is the case with our Dat lates). We offer a range of privacy information templates, including W nd an “offline” Privacy Notice.

Privacy information should ideally that is tailored to your audience. This is particularly important if yo ren’s personal data. In any case, you should aim to make your priva

- Clear (use plain language)
- Concise;
- Transparent; and
- Easily accessible.

It is also important to review priva o ensure that it is kept up to date. This is important when considerin data as a whole, not least where your lawful basis for using perso It is important to avoid “function creep” and not use personal d without adhering to the proper formalities. If your use of perso your privacy information must be updated to reflect this.

As noted above, *how* you obtai ermine *when* you should provide privacy information. It is also impo even if you are obtaining personal data from a third-party source rat ubjects themselves, you must still provide your own privacy informa you are gathering personal data from publicly accessible sources.

If you intend to use personal dat to that for which it was originally obtained, ensure that your privacy ut this. Similarly, if personal data is obtained from a publicly availa e of personal data is likely to be unexpected or intrusive to data su privacy information provides clear details about what you are doing.

Exceptions

There are limited exceptions to the vacy information. When collecting personal data directly from data s e to furnish them with information that they already have.

When collecting personal data via t need to furnish the data subject with privacy information in the follo

- They already have the req
- It would be impossible to or would involve disproportionate effort;
- The achievement of the o ng of the personal data would be rendered impossible or ser re to provide the information;
- You are obtaining or disclo comply with a legal obligation; or
- You are under an obligatio y regulated by law that covers the personal data in question.

SAMPLE

Part 2. The Right of Acces

This right is another important co ency principle. Data subjects have the right to access the personal t them. This right is exercised by means of a subject access reque d as “SAR” (also known as a data subject access request or DSAR).

A SAR does not need to follow a n be made orally or in writing. As with most of the other rights detail tes, strict time limits apply to your response. It is therefore importa your organisation who is likely to receive a SAR knows how to ect Access Request Policy and Procedure can assist in this regar

Generally speaking, you have o respond to a SAR and, in most cases, must do so free of charge. these rules, but they will likely not apply in most cases.

Your response to a SAR should i you are processing personal data about the data subject, a copy o d certain other information which mostly matches that which you sh privacy information.

As noted above, SARs do not n ular format. Training your staff to recognise SARs is therefore impo quired to do so, you can also help make things easier for data sub f by providing a Subject Access Request Form (but you cannot *re*

Please Refer to our Subject Access R

The right of access can, at times x. We have provided a dedicated set of Guidance Notes on SARs the proper calculation of the time limit for response, exceptions, thir e.

A range of template letters for res available.

SAMPLE

Part 3. The Right to Rectifi

If personal data is inaccurate or i jects to whom that personal data relates have the right to have it r Vhereas the first two rights relate closely to the principle of transpar n the accuracy principle.

When a request for rectification eed to take *reasonable steps* to determine whether the personal d te (or complete) and to correct it if necessary. Generally speaking, t hat the data is correct, the more work you should put into makin ill be a key consideration when determining what is "reasonable" have already taken to verify the accuracy of the personal data. At rtant to remember that you should have already taken steps to ens e and up to date, in line with the principles set out in Article 5 of the

As with other requests to exercis ere is no specified form for data subjects to follow. A request ca n writing to anyone within your organisation. Training your staf est is therefore very important, particularly given the tight time c challenges the accuracy of their personal data and asks you to co mplete incomplete personal data, it is a valid request.

Inaccurate Data or a Matter of Opinio

According to the Data Protection is inaccurate if it is "incorrect or misleading as to any matter of fa n, it will be clear whether or not personal data is accurate – an o hat happens, however, where the data in question is subjective, i.e.

According to the ICO:

> As long as the record sho mation is an opinion and, where appropriate, whose e difficult to say that it is inaccurate and needs to be

A data subject may still object to er of reasons, but data protection law is likely not the best vehicle by

Inaccurate Data or a Mistake?

Personal data will often be inaccu ere may, however, be times when the personal data in question ma ake that has since been fixed. In such cases, to "rectify" the data nce to the mistake would not be appropriate. Again, what is impo whether or not personal data is inaccurate is whether or not it is *in to any matter of fact*.

Restricting Contested Data

Part 5 of these Guidance Notes e ct processing. This right is closely connected to the right to rectific has challenged the accuracy (or completeness) of personal data, restrict your processing of that personal data while you are verify a subject may expressly exercise their right to restrict processing, bu a good idea to do it.

Resolving the Matter

If, after consideration of the data determine that the personal data does need to be corrected, you sh But what if you determine that it is accurate? An explanation should ject along with information about their right to complain to the ICO c rights through a judicial remedy.

SAMPLE

The Time Limit for Response

The time limit for responding to ne month from the receipt of the request. Care must be taken whe l as it is not quite as simple as it may first appear.

First of all, there are limited ext nth period if you have requested information to confirm the identi king the request or if you have requested a fee. In these circu it begins when you receive the information and/or fee but you mu n that crucial first month of receipt of the request itself.

Secondly, there is the matter of ca he time limit should be calculated from the day you receive the rec to the corresponding day in the following month. What if there is r the following month? In this case, the period ends on the last day of

For example, the normal time lin d on 5 January would end on 5 February. The time limit for a requ ary, on the other hand, would end on 28 February (or 29 February in

What about weekends or public he time limit extends to the next working day if it would otherwise e lic holiday.

In light of such complications, ther nds setting an internal time limit of 28 days for response so as to ens kenly exceed the legal time limit.

In some limited circumstances, it i one-month time limit by up to two months. This only applies if a re you have received a number of requests from the same person. If ary, you must inform the individual within the first month, giving your r .

Charging a Fee

In most cases, you cannot charg to any request to exercise data subject rights. If, however, a reque ded or excessive", you can charge a fee sufficient to cover the admin ng with that request.

You also have the option of refu anifestly unfounded or excessive request (see below).

Note that if you charge a fee, you d be in a position to explain to the ICO as well, if required). You shou ta subject that they have the right to complain to the ICO and that t orce their rights through a judicial remedy.

Verifying Identity

If you have "reasonable doubts" person making the request, you may request additional informatior dentity of the data subject.

Note that if you ask for such info lain why (and be in a position to explain to the ICO as well, if requi plain to the data subject that they have the right to complain to the y be able to enforce their rights through a judicial remedy.

Refusing to Comply

In some cases, you may be able t a request to exercise data subject rights on the grounds of an exemp dly into the following categories:

- Crime, law, and public prot
- Regulation, parliament, an

SAMPLE

- Journalism, research, and
- Health, social work, educa
- Finance, management, an
- References and exams; a
- Information about others i ss requests.

These exemptions fall outside the ce Notes. If you think that one or more may be relevant to your please contact the ICO or seek professional legal advice.

It is also possible to refuse to hat are manifestly unfounded or excessive. Note that if you refuse xplain why (and be in a position to explain to the ICO as well, if requ plain to the data subject that they have the right to complain to the y be able to enforce their rights through a judicial remedy.

What is Manifestly Unfounded?

The ICO explains that a request if the data subject clearly has no actual intention of exercising the ay, for example, make a request and then offer to withdraw it in exc enefit from you.

Similarly, a request may be manif licious in intent and is being used to harass your organisation with an to cause disruption. Examples include:

- The person making the stated that they intend to cause disruption;
- The request makes unsub gainst you or specific members of your team;
- The person making the re ular member of your team against whom they have a persona
- The person making the re nding different requests to you on a regular basis with the int on.

Refusing to comply with a reque it is manifestly unfounded is not something to be taken lightly a simple box-checking exercises (although it would seem that so obvious than others). Each case should be assessed on its own a in mind that even an apparently *aggressive* request may still be , even if the same person has previously made manifestly unfou not mean that any new ones can be automatically deemed manifes uestion is whether or not the data subject truly wants to exercise the

What is Excessive?

A request is considered excessiv ance of previous requests and it either overlaps with such request as not passed since receipt of the previous requests.

As with manifestly unfounded re ts must be considered on a case by case basis, taking into account es.

As the ICO explains, the follow utomatically constitute excessive requests:

SAMPLE

- The person making the r made a request about the same issue;
    - There may be legiti such requests again.
- The person making the re ping request, but one that relates to a different set of persona
- The person making the made manifestly or unfounded requests.

Informing Other Parties of Rectificatio

If personal data that is rectified en shared with another recipient (including an individual, organisa gency, or other body), you must inform such recipients of the uld be impossible or involve disproportionate effort to do so also be informed about such recipients.

SAMPLE

Part 4. The Right to Erasur

This right gives data subjects the ta erased. It is also known as *the right to be forgotten*. At the outset at this is not an absolute right and that it only applies in the following

- It is no longer necessary f nal data in light of the purpose(s) for which it was originally c
- You are using consent as g the personal data and the data subject withdraws their cor
- You are using legitimate i basis for using the personal data, the data subject has exerc (see Part 7, below), and there is no overriding legitimate int tinue;
- You are processing the p marketing purposes and the data subject objects to that proc
- You have used the person
- You are required to erase ply with a legal obligation; or
- You have processed the p offer information society services to a child.

Following on from the final point, i relates to personal data collected from children, the ICO states th ticular weight to any request for erasure if the processing is bas by a child…" This is particularly important as children may not b sequences of handing over their personal data and of the risks inv also be taken even where the data subject in question is no longer a ersonal data was provided to you when they were.

As with other requests to exercis ere is no specified form for data subjects to follow. A request ca n writing to anyone within your organisation. Training your staff st for erasure is therefore very important. If the request satisfies c bove, it is a valid request.

Erasing Personal Data

The word "erasure" tends to poin , but it is important to remember that personal data may also be st

Erasing Electronic Personal Data

When erasing electronic data, it i ind that simply deleting it will not necessarily remove it from a stora rd disk. The deletion often occurs only at the software level, but unti disk is overwritten with new data, the magnetic storage itself rema once data has been overwritten, erasing electronic data beyond r without physically destroying the storage medium, as sophisticate an be used to restore data even where it has been overwritten in unless the personal data is highly sensitive (most likely to a degre SMEs), deleting the data in the normal way is likely to be sufficien

Options for deleting data stored el

- Physical destruction of sto for removable media such as CD and DVD ROMs, but for drives, this can be an expensive option. Extreme methods i g hard disks to dust; however, this is likely to be unnecessary dled by SMEs.

SAMPLE

- Secure deletion – rather t , this method involves overwriting the sectors of the disk o stored with new data. The more 'passes' that are made, th on. Typical methods range from a single pass of zeroes, to mized data. It is important to be aware, however, that this not always an option with newer forms of storage such as S due to the way in which they store data. Many SSDs have th software, and increasingly, there are third-party applicatio if full and secure erasure is something you wish to co keep in mind when choosing your storage devices.
- Other methods include re device to factory settings and/or formatting the drive. It is i wever, that unless such methods are combined with secure fer any more security than simply deleting the individual files

Such methods are important for ut in most cases, particularly for SMEs, what is realistically impor nal data "beyond use". Guidance from the ICO defines "beyond use

> The ICO will be satisfied n 'put beyond use', if not actually deleted, provided olding it:
>
> - is not able, or will r ersonal data to inform any decision in respec a manner that affects the individual in any wa
> - does not give any c to the personal data;
> - surrounds the p propriate technical and organizational secu
> - commits to perma rmation if, or when, this becomes possible.

Clearly, then, the more permane the better; however, you are not expected to physically destroy y the Information Commissioner's Office guidance on deletion clearl):

> If you delete an item to yo 'quick format' of your hard drive or perform a factory u will be typically deleting data. However, data reco this data. **Even with that said, data deletion is e method of removing personal data from a dev**

In short, therefore, selecting the e, deleting it, and emptying your *Recycle Bin* or *Trash*, will ge particularly for SMEs handling comparatively low-risk personal d re is any doubt, specialist advice should be sought and there are n roviders who offer secure erasure services at a range of levels.

Erasing Physical Personal Data

While much information used in electronically, paper records still exist, more so in some contexts ases where your primary form of personal data storage is electroni eep track of printed copies and to ensure that such copies are destr ctronic counterparts are deleted.

When disposing of hardcopy reco to avoid any personal data being recognizable after disposal. It is, t me that simply throwing the paper

SAMPLE

into the recycling bin will not be s st, physical records incorporating personal data should be shredded

When selecting a suitable shredd ep in mind that different levels of security are available, some in co DIN security levels which run from 1 to 6 with 1 being the least secu DIN 1, for example, shreds paper into strips a maximum of 12mm w y be suitable for home use. At the other end of the scale, DIN 6 shre to a particle size of 0.8mm v 4mm and are generally used for govern tions. DIN 2 at a minimum, or DIN 3 shredders are generally more s , but specialist advice should be sought if there is any doubt.

Erasing Backups

When considering your obligatio quest for erasure, it makes no difference whether data is stored backup. It must be erased unless an exemption applies that release n. As the ICO explains, however, the steps that you must take t sonal data "will depend on your particular circumstances, your ret e technical mechanisms that are available to you".

Furthermore, the ICO points out th

> It may be that the erasure y fulfilled in respect of live systems, but that the data backup environment for a certain period of time until

As noted above, what matters i ata is put "beyond use", even in situations where it cannot be ove The data should not be used and merely held on your backup syste accordance with a set schedule. While conceding that the risk is s rticular context, the ICO suggests that this is unlikely to pose a signif

Exemptions to the Right to Erasure

If the processing of the persona cessary for one of the following purposes, the right does not apply

- For exercising the right to f d information;
- For complying with a legal
- For the performance of a ublic interest or in the exercise of official authority;
- For archiving purposes in tific research, historical research, or statistical purposes whe a is likely to render the processing impossible or seriously imp
- For the establishment, exe claims.

The UK GDPR also sets out two h relate to special category data, specifically that relating to health. ect these to apply to most SMEs, they are included here for complet

- The processing of the per for public health purposes in the public interest; or
- The processing of the pers or the purposes of preventative or occupational medicine. T only where the data is being processed by or under the essional who is subject to a legal obligation of professional s professional.

SAMPLE

In some cases, you may be able t a request to exercise data subject rights on the grounds of an exemp dly into the following categories:

- Crime, law, and public prot
- Regulation, parliament, an
- Journalism, research, and
- Health, social work, educa
- Finance, management, an
- References and exams; an
- Information about others in ss requests.

These exemptions fall outside the ce Notes. If you think that one or more may be relevant to your lease contact the ICO or seek professional legal advice.

It is also possible to refuse to hat are manifestly unfounded or excessive. Note that if you refuse xplain why (and be in a position to explain to the ICO as well, if requi plain to the data subject that they have the right to complain to the y be able to enforce their rights through a judicial remedy.

What is Manifestly Unfounded?

The ICO explains that a request if the data subject clearly has no actual intention of exercising the ay, for example, make a request and then offer to withdraw it in exc enefit from you.

Similarly, a request may be manif licious in intent and is being used to harass your organisation with an to cause disruption. Examples include:

- The person making the stated that they intend to cause disruption;
- The request makes unsub gainst you or specific members of your team;
- The person making the red ular member of your team against whom they have a persona
- The person making the red nding different requests to you on a regular basis with the int on.

Refusing to comply with a reque it is manifestly unfounded is not something to be taken lightly a simple box-checking exercises (although it would seem that so obvious than others). Each case should be assessed on its own a in mind that even an apparently *aggressive* request may still be even if the same person has previously made manifestly unfou not mean that any new ones can be automatically deemed manifes uestion is whether or not the data subject truly wants to exercise the

What is Excessive?

A request is considered excessiv ance of previous requests and it either overlaps with such requests as not passed since receipt of the previous requests.

SAMPLE

As with manifestly unfounded req ts must be considered on a case by case basis, taking into account es.

As the ICO explains, the follow utomatically constitute excessive requests:

- The person making the r made a request about the same issue;
    - There may be legiti such requests again.
- The person making the re ping request, but one that relates to a different set of persona
- The person making the made manifestly or unfounded requests.

The Time Limit for Response

The time limit for responding to a rmally one month from the receipt of the request. Care must be take period as it is not quite as simple as it may first appear.

First of all, there are limited ext th period if you have requested information to confirm the identi king the request or if you have requested a fee. In these circu it begins when you receive the information and/or fee.

Secondly, there is the matter of c he time limit should be calculated from the day you receive the rec to the corresponding day in the following month. What if there is r the following month? In this case, the period ends on the last day of

For example, the normal time lin d on 5 January would end on 5 February. The time limit for a requ ary, on the other hand, would end on 28 February (or 29 February in

What about weekends or public he time limit extends to the next working day if it would otherwise e lic holiday.

In light of such complications, ther nds setting an internal time limit of 28 days for response so as to ens kenly exceed the legal time limit.

In some limited circumstances, it one-month time limit by up to two months. This only applies if a re you have received a number of requests from the same person. If ary, you must inform the individual within the first month, giving your r .

Charging a Fee

In most cases, you cannot charg to any request to exercise data subject rights. If, however, a reque ded or excessive", you can charge a fee sufficient to cover the admin ng with that request.

You also have the option of refu anifestly unfounded or excessive request (see above).

Note that if you charge a fee, you d be in a position to explain to the ICO as well, if required). You shou ta subject that they have the right to complain to the ICO and that t orce their rights through a judicial remedy.

SAMPLE

Verifying Identity

If you have “reasonable doubts” person making the request, you may request additional informatio dentity of the data subject.

Note that if you ask for such info lain why (and be in a position to explain to the ICO as well, if requ plain to the data subject that they have the right to complain to the y be able to enforce their rights through a judicial remedy.

Informing Other Parties of Erasure

If personal data that you are requ isclosed to another party or if that personal data has been made pu nment (e.g. on social media or a website), you must inform the othe

In the first case, each specific med of the erasure unless it is impossible or would involve disp so. Data subjects must also be informed about these parties if you

In the second case, “reasonable s nt available technology and costs) must be taken to inform other data cessing the affected personal data to erase links to it, as well as copie

SAMPLE

Part 5. The Right to Restric

In certain circumstances, data su you limit the ways in which you process their personal data. This esting erasure, and data subjects will make a request of this kind Restrictions do not generally last indefinitely.

The right to restrict processing ap umstances:

- The data subject has cha their personal data (see Part 3, above) and you are in the curacy;
- You have processed the , but the data subject wants the processing of their person than having the data erased (see Part 4, above, for the right
- You do not need the perso e data subject needs you to hold onto it in order to establish gal claim; or
- The data subject has obje f their personal data (see Part 7, below) and you are in the whether your legitimate grounds override the data subject's

With respect to verifying accuracy ection, the ICO recommends that you automatically restrict your p d personal data as a matter of course, rather than waiting for the

As with other requests to exercis ere is no specified form for data subjects to follow. A request ca n writing to anyone within your organisation. Training your staff to restrict processing is therefore very important. If the request relat set out above, it is a valid request.

Restricting Processing of Personal Da

Firstly, it is important to keep in m defined by data protection law is a very broad term and covers just u do with the data. Indeed, even erasing data is a form of processin

How to restrict the processing of d upon what kind of data you are dealing with, what you are alread re and how it is stored. While the method of restriction will vary f ever, the UK GDPR makes the following suggestions:

> Recital 67
>
> Methods by which to r of personal data could include…temporarily movi nother processing system, making the selected per to users, or temporarily removing published data mated filing systems, the restriction of processing sh ured by technical means in such a manner that the p ject to further processing operations and cannot be he processing of personal data is restricted should be system.

Is there anything that you *can* do data? Generally speaking, no, but there are some very limited excep

- You have the data subject' g with it;
- You need to process the p blishment, exercise, or defence of legal claims;

SAMPLE

- The processing is necessa another (natural or legal) person's rights; or
- The processing is necessa erest reasons.

Removing Restrictions

If the processing of personal da u are assessing the accuracy of personal data (where the data su right to rectification) or where the data subject has objected to you g on public interest or legitimate interests grounds) and you are c r legitimate interests override the data subject's, the restriction wi ry. Once the accuracy issue is resolved or you have determined unds override the data subject's, the restriction may be lifted.

It is important, in such circumsta idual that the restriction is being lifted before you lift it. If you are n a (i.e. you have determined that it is accurate), you should inform th asons. Likewise, if you determine that your legitimate grounds over you should explain your reasons. When doing so, it is also importan a subject of their right to complain to the ICO and to seek a judicial re

Refusing to Comply

In some cases, you may be able t a request to exercise data subject rights on the grounds of an exemp dly into the following categories:

- Crime, law, and public prot
- Regulation, parliament, an
- Journalism, research, and
- Health, social work, educat
- Finance, management, an
- References and exams; an
- Information about others in ss requests.

These exemptions fall outside the ce Notes. If you think that one or more may be relevant to your please contact the ICO or seek professional legal advice.

It is also possible to refuse to hat are manifestly unfounded or excessive. Note that if you refuse xplain why (and be in a position to explain to the ICO as well, if requi plain to the data subject that they have the right to complain to the y be able to enforce their rights through a judicial remedy.

What is Manifestly Unfounded?

The ICO explains that a request if the data subject clearly has no actual intention of exercising the hay, for example, make a request and then offer to withdraw it in exc enefit from you.

Similarly, a request may be manif licious in intent and is being used to harass your organisation with an to cause disruption. Examples include:

- The person making the stated that they intend to cause disruption;

SAMPLE

- The request makes unsub gainst you or specific members of your team;
- The person making the rec ular member of your team against whom they have a persona
- The person making the rec nding different requests to you on a regular basis with the int on.

Refusing to comply with a reque it is manifestly unfounded is not something to be taken lightly a simple box-checking exercises (although it would seem that so obvious than others). Each case should be assessed on its own a in mind that even an apparently *aggressive* request may still be even if the same person has previously made manifestly unfou not mean that any new ones can be automatically deemed manifes uestion is whether or not the data subject truly wants to exercise the

What is Excessive?

A request is considered excessiv ance of previous requests and it either overlaps with such request as not passed since receipt of the previous requests.

As with manifestly unfounded req ts must be considered on a case by case basis, taking into account es.

As the ICO explains, the follow utomatically constitute excessive requests:

- The person making the r made a request about the same issue;
    - There may be legiti such requests again.
- The person making the re ping request, but one that relates to a different set of persona
- The person making the made manifestly or unfounded requests.

The Time Limit for Response

The time limit for responding to is normally one month from the receipt of the request. Care must ng this period as it is not quite as simple as it may first appear.

First of all, there are limited ext th period if you have requested information to confirm the identi king the request or if you have requested a fee. In these circu it begins when you receive the information and/or fee.

Secondly, there is the matter of c he time limit should be calculated from the day you receive the rec to the corresponding day in the following month. What if there is r the following month? In this case, the period ends on the last day of

For example, the normal time lin d on 5 January would end on 5 February. The time limit for a requ ary, on the other hand, would end on 28 February (or 29 February in

What about weekends or public he time limit extends to the next working day if it would otherwise e ic holiday.

SAMPLE

In light of such complications, ther nds setting an internal time limit of 28 days for response so as to ens kenly exceed the legal time limit.

In some limited circumstances, it i one-month time limit by up to two months. This only applies if a re you have received a number of requests from the same person. If ary, you must inform the individual within the first month, giving your r .

Charging a Fee

In most cases, you cannot charg to any request to exercise data subject rights. If, however, a reque ded or excessive", you can charge a fee sufficient to cover the admin ng with that request.

You also have the option of refu anifestly unfounded or excessive request (see above).

Note that if you charge a fee, you d be in a position to explain to the ICO as well, if required). You shou ta subject that they have the right to complain to the ICO and that t orce their rights through a judicial remedy.

Verifying Identity

If you have "reasonable doubts" person making the request, you may request additional informatior dentity of the data subject.

Note that if you ask for such info lain why (and be in a position to explain to the ICO as well, if requi plain to the data subject that they have the right to complain to the y be able to enforce their rights through a judicial remedy.

Informing Other Parties of Restriction

If personal data subject to a reque essing has been shared with other parties, you must inform each p unless it is impossible or would involve disproportionate effort to uld also be informed about such recipients.

SAMPLE

Part 6. The Right to Data P

If your lawful basis for processin sent, or for the performance of a contract, and the processing of th ed out by automated means, data subjects have the right to receive "structured, commonly used, and machine-readable format", and (or, where feasible, to have it transmitted) that data to another o

The idea behind this right is to a ove their personal data between different services without its usabi

It is important to note that, in addi (i.e. consent or contract), the right applies only to personal data that vided to you. This is an important point and is not quite as simple as

As with other requests to exercis ere is no specified form for data subjects to follow. A request ca n writing to anyone within your organisation. Training your staff st to exercise the right to data portability is therefore very importa

When is Personal Data Provided to Y

In some cases, this will be ob ere the data subject gives you information directly when registeri milar. The definition goes beyond this, however and also includes p from your observation of the data subject's activities.

Examples of such data include:

- Website usage history or s
- Traffic and location data; o
- Raw data from connected wearables and smart metres.

What this definition does not inclu created *based upon* data provided by the data subject. It is importan while any such personal data isn't covered by the right to portability ht of access (see Part 2, above). Consequently, the ICO still recom

> …if it is clear that the in ss to the inferred/derived data, as part of a wider ould be good practice to include this data in your re

Anonymised and Pseudonymised Per

If personal data is truly anonym portability does not apply. If it is pseudonymised and can be conne the right does apply.

Personal Data About Multiple Data Su

If information covered by a rec y includes personal data about someone other than the data s will need to determine whether providing the information would hts and freedoms of the others involved. Generally, the ICO sugg data to the individual making the request "should not be a problem party information in question was provided to you by that individu It is still important, however, to consider the rights and freedoms

If, on the other hand, personal d by multiple data subjects, for example, when setting up a join sure that they all agree to the portability request and may need t ement.

SAMPLE

Complying with a Request

Where the right to data portabili s are entitled to a copy of their personal data and/or to have it se (data controller).

When it comes to providing the data subjects, this can be done either directly in response to a right to data potability, or more proactively by providing access to -service system. Whichever route you take, ensuring security is impo

If the data subject asks you to s directly to another controller, you must do so if it is technically fe ally obliged to adopt or maintain systems that are compatible with rganisations simply because this right exists, but you should be re echnology, formats, and so forth. Given the range of widely-used data formats available, it should arguably not be difficult to ensure mostly compatible with others, at least where the data itself is conce

Data protection law also requires accordance with this right "without hinderance", i.e. you should not echnical, or financial obstacles in the way of the process. That said t there are not legitimate grounds for being unable to transmit data ist advice should be sought from the ICO or a suitably qualified lega

As noted above, security is impo it comes to transmitting personal data in response to a request for responsible for the transmission itself, whether to the data subje sation. You are not responsible, however, for the use that the pers it is in the other party's hands. It can be helpful, however, particula o individuals, to provide guidance on keeping personal data safe an

How to Provide the Personal Data

When complying with a request onal data must be provided in a format that is:

- Structured;
- Commonly used; and
- Machine-readable.

It may also make things easier to s. If you work in a particular sector or industry where data sharing in , it can be advantageous to all to work together to ensure the adopt ats for personal data.

You are not required by law to us ely. You may need or want to use proprietary formats internally whic or usable by individuals or other organisations. You will, however, s possible to convert data into an open format when complying wit bility. Popular open formats that meet the above requirements inclu N.

There is no prescriptive or exhaus should be used, but these formats are likely to be widely usable. however, to take account of the recipient and the technologies ava cases, even formats that meet the above criteria may not be access hough, in practice, in most cases they will be, even if an individual o c laptop or smartphone.

Receiving Personal Data Transmitted rtability

So far, these Guidance Notes h from the perspective of a data controller *sending* personal data another organisation, but what happens when you are on the *rec*

SAMPLE

You must, firstly, determine whetl hold on to the data. Ask yourself whether or not the data is relev is not excessive in light of the purpose(s) for which it will be proc any personal data relating to third parties.

If third party data is involved, you or not you have a reason to keep it and, if so, what your lawful bas ping so and for processing it. You must also ensure that your proces affect the rights and freedoms of the data subjects concerned.

It is particularly important to note t ses:

> …if you receive third pa t use this for your own purposes. You should kee der the sole control of the individual who has made t nd only used for their own purposes.

Refusing to Comply

In some cases, you may be able t a request to exercise data subject rights on the grounds of an exemp dly into the following categories:

- Crime, law, and public prot
- Regulation, parliament, an
- Journalism, research, and
- Health, social work, educa
- Finance, management, an
- References and exams; ar
- Information about others in s requests.

These exemptions fall outside the ce Notes. If you think that one or more may be relevant to your please contact the ICO or seek professional legal advice.

It is also possible to refuse to hat are manifestly unfounded or excessive. Note that if you refuse xplain why (and be in a position to explain to the ICO as well, if requi plain to the data subject that they have the right to complain to the y be able to enforce their rights through a judicial remedy.

What is Manifestly Unfounded?

The ICO explains that a request if the data subject clearly has no actual intention of exercising the ay, for example, make a request and then offer to withdraw it in exc enefit from you.

Similarly, a request may be manif licious in intent and is being used to harass your organisation with n an to cause disruption. Examples include:

- The person making the r stated that they intend to cause disruption;
- The request makes unsub gainst you or specific members of your team;
- The person making the red ular member of your team against whom they have a persona

SAMPLE

- The person making the req nding different requests to you on a regular basis with the int on.

Refusing to comply with a reque it is manifestly unfounded is not something to be taken lightly a simple box-checking exercises (although it would seem that so obvious than others). Each case should be assessed on its own a in mind that even an apparently *aggressive* request may still be even if the same person has previously made manifestly unfou not mean that any new ones can be automatically deemed manifes uestion is whether or not the data subject truly wants to exercise the

What is Excessive?

A request is considered excessiv ance of previous requests and it either overlaps with such requests as not passed since receipt of the previous requests.

As with manifestly unfounded req ts must be considered on a case by case basis, taking into account es.

As the ICO explains, the follow utomatically constitute excessive requests:

- The person making the r made a request about the same issue;
    - There may be legiti such requests again.
- The person making the re ping request, but one that relates to a different set of persona
- The person making the made manifestly or unfounded requests.

The Time Limit for Response

The time limit for responding to e month from the receipt of the request. Care must be taken whe as it is not quite as simple as it may first appear.

First of all, there are limited ext th period if you have requested information to confirm the identi king the request or if you have requested a fee. In these circu it begins when you receive the information and/or fee.

Secondly, there is the matter of c he time limit should be calculated from the day you receive the req to the corresponding day in the following month. What if there is r the following month? In this case, the period ends on the last day of

For example, the normal time lin d on 5 January would end on 5 February. The time limit for a requ ary, on the other hand, would end on 28 February (or 29 February in

What about weekends or public he time limit extends to the next working day if it would otherwise e ic holiday.

In light of such complications, ther nds setting an internal time limit of 28 days for response so as to ens kenly exceed the legal time limit.

SAMPLE

In some limited circumstances, it e one-month time limit by up to two months. This only applies if a f you have received a number of requests from the same person. sary, you must inform the individual within the first month, giving your n.

Charging a Fee

In most cases, you cannot cha g to any request to exercise data subject rights. If, however, a requ nded or excessive", you can charge a fee sufficient to cover the admi ing with that request.

You also have the option of ref manifestly unfounded or excessive request (see above).

Note that if you charge a fee, yo d be in a position to explain to the ICO as well, if required). You sho ata subject that they have the right to complain to the ICO and that force their rights through a judicial remedy.

Verifying Identity

If you have "reasonable doubts" e person making the request, you may request additional informatio identity of the data subject.

Note that if you ask for such inf plain why (and be in a position to explain to the ICO as well, if requ xplain to the data subject that they have the right to complain to th ay be able to enforce their rights through a judicial remedy.

SAMPLE

Part 7. The Right to Object

In limited circumstances, data su object to the processing of their personal data. In the case of dire bsolute right. In other cases, you may be able to override the object

Where personal data is process asons, the right to object is not absolute:

- A task carried out in the pu
- The exercise of official aut
- Your lawful basis is "legi processing is for the legitimate interests of a third party).

Further limitations to the right app ta is being processed for scientific research, historical research, or st

As with other requests to exercis ere is no specified form for data subjects to follow. A request ca n writing to anyone within your organisation. Training your staff to exercise the right to object is therefore very important.

Complying with the Right to Object

In the case of personal data used noted above, the right to object is absolute. There are, however, sor ep in mind. The right only applies to the extent that you are using th on for direct marketing. This does not mean that you must stop usin ng to that individual and delete it. There may be other purposes tha u may also suppress the personal data used for marketing rather t g that just enough information is retained to ensure that the data s targeted with direct marketing in the future.

In a situation where the personal processed for one of the following reasons, remember that the righ ata subject must provide specific reasons for their objection, based ation:

- A task carried out in the pu ;
- The exercise of official aut ic task); or
- Your lawful basis is "legi processing is for the legitimate interests of a third party).

If you can demonstrate "compe s" to continue processing which override the interests, rights, and bject; or the continued processing is necessary for the establishmen f legal claims, you may be able to refuse to comply with the request.

It will be important to consider w cting in this case. If, for example, they submit that the processing i ial damage or distress, it may be less likely that your interests will o e of this assessment means that it should not be taken lightly and t m the ICO or a suitably qualified legal professional should be soug

If you do conclude that you do n e request, you must tell the data subject and provide reasons for y also inform them of their right to complain to the ICO and their abili dy to enforce their rights.

SAMPLE

If you are processing personal d torical research, or for statistical purposes and have appropriate s a subjects only have the right to object if your lawful basis for proce is either:

- The exercise of official aut ic task); or
- Legitimate interests.

As above, you may nonetheless b ssing the personal data if you can demonstrate compelling legitima e processing or the continued processing is necessary for the es defence of legal claims.

Also as above, if you are satisfie to comply, you must tell the data subject and provide reasons for y also inform them of their right to complain to the ICO and their abili dy to enforce their rights.

The decision to erase personal da ise of the right to object will need to be taken on a case by case bas ted above, it will be wise to retain a small amount of data sufficient data relating to a particular data subject is not used for the same e.g. a "Do not mail" list). What is important, however, is that the per sed further.

As noted at the start of these Gui nform data subjects of the right to object. This must be done, at the mmunicate with the data subject. As should be clear from the info art 7, this applies where you are processing their personal data in t es:

- For direct marketing purpo
- On the "public task" lawfu ance of a task carried out in the public interest;
- On the "public task" lawful official authority vested in you; or
- On the "legitimate interests

The ICO also points out that the ght to object should be presented clearly and separately from other data is being used for research or statistical purposes, information a hould be included in your privacy information (see Part 1, above).

Other Reasons for Refusing to Comp

As with the other data subject righ refuse to comply with a request to exercise the right to object on t ption or because the request is manifestly unfounded or excessive

Exemptions fit broadly into the foll

- Crime, law, and public prot
- Regulation, parliament, an
- Journalism, research, and
- Health, social work, educa
- Finance, management, an
- References and exams; ar
- Information about others in s requests.

These exemptions fall outside the ce Notes. If you think that one or more may be relevant to your lease contact the ICO or seek professional legal advice.

SAMPLE

It is also possible to refuse to hat are manifestly unfounded or excessive. Note that if you refuse xplain why (and be in a position to explain to the ICO as well, if requi plain to the data subject that they have the right to complain to the y be able to enforce their rights through a judicial remedy.

What is Manifestly Unfounded?

The ICO explains that a request if the data subject clearly has no actual intention of exercising the ay, for example, make a request and then offer to withdraw it in exc enefit from you.

Similarly, a request may be manif licious in intent and is being used to harass your organisation with an to cause disruption. Examples include:

- The person making the stated that they intend to cause disruption;
- The request makes unsub gainst you or specific members of your team;
- The person making the red ular member of your team against whom they have a persona
- The person making the red nding different requests to you on a regular basis with the int on.

Refusing to comply with a reque it is manifestly unfounded is not something to be taken lightly a simple box-checking exercises (although it would seem that so obvious than others). Each case should be assessed on its own a in mind that even an apparently *aggressive* request may still be even if the same person has previously made manifestly unfou not mean that any new ones can be automatically deemed manifes uestion is whether or not the data subject truly wants to exercise the

What is Excessive?

A request is considered excessiv ance of previous requests and it either overlaps with such requests as not passed since receipt of the previous requests.

As with manifestly unfounded req ts must be considered on a case by case basis, taking into account es.

As the ICO explains, the follow utomatically constitute excessive requests:

- The person making the r made a request about the same issue;
    - There may be legiti such requests again.
- The person making the re ping request, but one that relates to a different set of persona
- The person making the made manifestly or unfounded requests.

SAMPLE

The Time Limit for Response

The time limit for responding to ne month from the receipt of the request. Care must be taken whe l as it is not quite as simple as it may first appear.

First of all, there are limited ext nth period if you have requested information to confirm the identi king the request or if you have requested a fee. In these circu it begins when you receive the information and/or fee.

Secondly, there is the matter of c he time limit should be calculated from the day you receive the rec to the corresponding day in the following month. What if there is r the following month? In this case, the period ends on the last day of

For example, the normal time lin d on 5 January would end on 5 February. The time limit for a requ ary, on the other hand, would end on 28 February (or 29 February in

What about weekends or public he time limit extends to the next working day if it would otherwise e lic holiday.

In light of such complications, ther nds setting an internal time limit of 28 days for response so as to ens kenly exceed the legal time limit.

In some limited circumstances, it i one-month time limit by up to two months. This only applies if a re you have received a number of requests from the same person. If ary, you must inform the individual within the first month, giving your r .

Charging a Fee

In most cases, you cannot charg to any request to exercise data subject rights. If, however, a reque ded or excessive", you can charge a fee sufficient to cover the admin ng with that request.

You also have the option of refu anifestly unfounded or excessive request (see above).

Note that if you charge a fee, you d be in a position to explain to the ICO as well, if required). You shou ta subject that they have the right to complain to the ICO and that t orce their rights through a judicial remedy.

Verifying Identity

If you have "reasonable doubts" person making the request, you may request additional informatio dentity of the data subject.

Note that if you ask for such info lain why (and be in a position to explain to the ICO as well, if requi plain to the data subject that they have the right to complain to the y be able to enforce their rights through a judicial remedy.

SAMPLE

Part 8. Rights Related to A Making including Profiling

Automated decision-making is a are made solely by automated means without any human involv law uses the phrase "automated decision-making including profilin often appear together, but not all automated decision-making will ne g.

Profiling, as defined by the UK GD

> Any form of automated pr a consisting of the use of personal data to evaluat ects relating to a natural person, in particular to a s concerning that natural person's performance a uation, health, personal preferences, interests, reli n or movements.

As this definition suggests, while aking does not necessarily mean profiling, the two will often be linke

Profiling is often used to find o le's preferences, to predict their behaviour, and to make decisions

The UK GDPR was designed, in p f automated decision-making and profiling. In particular, where solel ncluding profiling) have a "legal or similarly significant effect" on peo he right not to be subject to those decisions. Therefore, if a decision made without human involvement, it will be subject to restrictions and eria.

Such decision-making can only be

- It is necessary for the e nance of a contract between an organisation and the data s
- It is authorised by law; or
- It is based on the data sub

Furthermore, if special category (s involved, the circumstances are limited further:

- You have the data subject'
- The processing in questio ntial public interest reasons.

Managing Risk

Automated decision-making is c k". Before undertaking any such processing, a Data Protection Im e carried out. A Data Protection Impact Assessment or "DPIA" inv eration of a new proposed use of personal data, identifying risks an s that will solve or mitigate those risks.

Informing and Protecting Data Subjec

As explained above, transparen pect of modern data protection legislation such as the UK GDPR. mated decision-making, therefore, it is important that you provide cle ation about that processing to the individuals whose personal data ormation should explain the logic involved in the process and the si consequences of that process.

It is also required that you use " l or statistical procedures" in the process.

Technical and organisational me yed to correct inaccuracies and minimise the risks of errors arisin st be secured in a manner that is

SAMPLE

proportionate to the risks pose nd interests, and that prevents discriminatory effects.

Of particular importance in the co subject's rights, you must ensure that data subjects are able to ob express their point of view, and obtain and explanation of any dec d challenge that decision.

It is important to keep in mind tha aking process does not qualify as "solely automated decision-maki with legal or similarly significant effects", your processes must still ion law, including the principles of the UK GDPR. You must have a your use of personal data, which must be recorded; you must have t enable data subjects to exercise their rights; and you must remem e the right to object to profiling in certain circumstances and that thi r attention.

Automated decision-making and s and rights surrounding it, is a complex area and must not be tak ce should always be sought in the event that there is any doubt surro onal data in this manner.

SAMPLE