Privacy **Notes**

Introduction

In 2018, the EU General Data Pro monly known simply as the GDPR represented a significant modernis aw and one that took into account significant new developments in tec of personal data that simply did not exist at the time of the previous le ction Act 1998. Following the UK's departure from the European Uni ertain contextual alterations which change little from an SME perspe law by virtue of section 3 of the European Union (Withdrawal) Act 2 s the "UK GDPR". Together with the Data Protection Act 2018, the UK ne of UK data protection legislation (in addition to other important la y and Electronic Communications Regulations). These pieces of legis ely referred to in legal and business documents as "the Data Protection

Note that these Guidance Notes co compliance. If you process personal data relating to individuals outside o (such as the EU GDPR) will apply.

At the core of the UK GDPR are the , fairness, and transparency. Under these principles, you must have a collecting, holding, and processing personal data, you must only use it law itself, and you must only use it fairly, i.e. it should not be used in a mental to individual data subjects, or in any way that is unexpected or mis

Of central importance to these Gui ciple of transparency, which is itself closely related to the individual "R der the UK GDPR. This essentially envelops all of the above, as you about the personal data you are collecting from (or about) them, the which you are using that data, how long you will hold it, and who (if any .

This all-important "Privacy Informati a manner that is easily accessible to individuals, meaning that you s plain language to concisely and transparently convey everything tha s. This, it must be conceded, is not always easy because of the s mation that the Data Protection Legislationrequires you to provide. have been designed to set out the information required, to explain tha nd to provide a practical context in order to assist in completing your ov

Privacy Information can be found u ames. Some have a *Privacy Policy*; others prefer a *Privacy Notice* or a at is important is that it is clear to individuals where to find the infor is less important. In Simply-Docs' case, we call our website privacy in *acy Policies* and our offline (or non-website) equivalents *Privacy Notice* s are used only to differentiate.

Part 1. The Information Re

Whatever you decide to call it, your include the following:

- The name and contact detai
  - It is important that da using their personal data.
- The name and contact detai (if applicable):
  - If you provide produc r the behaviour of individuals in the EEA but are based you must appoint an EEA-based representative. As of apply to businesses in the UK.
- The contact details of your d ou have one):
  - Some organisations data protection officer by law. Even if you are not require free to do so (and it can be a good idea to have a sing d responsibility for data protection matters).
- Details about the personal d
  - It is important to cor definition of "personal data" when providing this inform personal data is 'any information relating to an identif l person. An identifiable person is one who can be iden y, by reference to an identifier such as a name, an identi data, online identifier, or to one or more factors specific logical, genetic, mental, economic, cultural, or social ide ine identifiers in particular are likely to be a common form ed by many businesses.
- Details about how you collec
  - In many cases, this v context. Personal data collected, for example, via an onli ign up to a website or via a paper order form at your clear to the individual. Less clear, however, is data coll s such as that collected via cookies and similar technolo rmation should cover this. If you collect personal data you explain how, whether it seems obvious to you or not
- The purpose or purposes for onal data:
  - Individuals have a ri ll use their personal data and your purposes for collecti ensure that you clearly identify the purpose(s) for whic sonal data and ensure that those purposes are lawful a
- The lawful basis or bases on s personal data:
  - A range of lawful you under the Data Protection Legislation, including ocess personal data in relation to a contract, compliance performance of a task in the public interest or for official interests (the most flexible choice).

- Your legitimate interests fo data (if this is your chosen lawful basis):
    - This is a flexible bas ersonal data processing is justified. Care must be taken, it is a valid choice. This not a *one-size-fits-all* solution a uited to uses of personal data that individuals are reaso d which have a minimal impact on their privacy. Detail rests you are relying on must be provided to individua
- Where personal data is obta ather than the individual to whom it relates, the category or cate
- Details of any third parties t sonal data (the recipients or at least the categories of recipient):
    - While it may not al ossible to provide full information, providing as much de s heading is good for transparency. If possible, it is a go to the privacy notices or policies of those third parties.
- Details of any transfers of pe ountries (known as “third countries”) or to international organisati
    - It is important to kee beyond direct transfers of personal data and can includ ectronically by a third party service provider in a non-UK g data available to an organisation situated outside the U
    - From 1 January 202 EU perspective, is a third country. At present, transfers of e UK to the EEA are permitted as before. Furthermore e EU-UK Trade and Cooperation Agreement, EEA to continue to be permitted during a temporary period of ding an EU Commission adequacy decision as to the UK tion.
    - You should also sta mechanism applies, whether it is anadequacy decisio clauses, binding corporate rules, individual consent, d of the Brexit transition period, transitional provision sting EU adequacy decisions and approved safeguards gnised in the UK. The UK will also be able to make it ions (“adequacy regulations”) and approve further safe , that during the temporary period mentioned under th decisions and safeguards will be subject to EU appro nlikely to significantly impact your choices as a busine ommissioner’s Office is unlikely to provide details of suc re approved and ready to use.)
- Your retention periods for p tention will be determined if certain personal data does not have set in advance):
    - Always remember th d to keep personal data for as long as you need it in lig rpose(s) for which it was originally collected. For some re fixed by law, but in many cases, you will need to make elf.

- Details of individual data sub for in the UK GDPR including those relating to the processing their right to withdraw consent (if consent is your lawful basis data), and their right to complain to the Information Commission
    - Individuals have a ne lawand part of your job when providing Privacy Inf ights out, along with details on how to exercise them. Wh easy mechanisms such as controls, preferences, or easy als to exercise their rights can be a positive step.
- Where personal data is obta ather than the individual to whom it relates, details of the source
- Details of any legal obligatio under to provide personal data, i.e. a statutory obligation or a c ny possible consequences of failing to provide that personal data
- If you carry out automated ng profiling) on the personal data, details of that processing in mation about the logic involved and the envisaged consequence e individual data subject.

As noted above, you must provide cise and user-friendly manner. It is also important to consider *when* to p on.

If you are collecting personal data d s, you should supply this information at the time of collection. This appro nline with privacy policies or privacy statements that users are required t signing up to a website.

If, on the other hand, you are collec rty, it will not be possible to provide Privacy Information to the individua d at the time of collection. Instead, you must provide the information as

- Within a reasonable period o data from the third party and, in any case, no more than one mon
- If you intend to communica , when your first communication is made, at the latest; or
- If you intend to disclose the r party, when that personal data is disclosed, at the latest.

It is also important to ensure that y can be easily accessed at all times. Many websites, for example, have l y and their terms and conditions on every page. Such links are generally however, it is worth keeping in mind that if a page contains a large amo uiring users to scroll a long way to reach the footer, that this approach accessible" aspect of your Privacy Information. Design, page layout, xperience are therefore important considerations alongside the actua cy Information when presenting it online.

Note also that if you are providing s should provide links to the relevant privacy information in the applica platforms including iOS, Android, Windows, and macOS allow publish ks to their privacy policies from app

pages in their respective stores. T individuals can read your Privacy Information before downloading an also important to ensure that your Privacy Information is accessible fro oo.

Unsurprisingly, a great deal ofinfo GDPR focuses on privacy online. Thought may also need to be giver vacy Information on your premises. In some cases, it may be appropri formation alongside documentation designed to collect data. In other ca notice in clear view of, for example, your reception desk or till can be h if you do not collect personal data through your website or offer any merce, putting your “offline” privacy notice on your website can be a goo ccessibility for your customers.

The next question is how to presen duals, ideally without overwhelming them. The Information Commissione owing suggestions:

- A layered approach – split into short sections which can be expanded or collapsed, ther vigation and reducing the likelihood of information overload by p large bodies of endless text;
- Dashboards – privacy prefer individuals how their personal data will be used and how they d suggest that providing everything required in this way would b
- Just-in-time notices – focu delivered at the time you collect specific pieces of informatio could work better in some scenarios than others as many organis all data at the same time);
- Icons – used, in essence, t of particular types of personal data processing; and
- Mobile and smart device ample, pop-ups, voice alerts, and gestures.

While it is clear that the Information s trying to suggest a range of helpful methods that make complying wit ed and the transparency principle easier for all concerned, it is perha ow some of their suggestions could work in practice. Your mileage, of c

Part 2. Background - The R ed

This is what you're doing it all for. T over-arching principle, but providing the required Privacy Information to e, your fulfilment of their right to be informed.

The right to be informed is set out i he UK GDPR and, as noted above, ties in directly with the principle o ole of the UK GDPR is improving accountability, ensuring that individu their personal data, and – as is the focus here – ensuring that they hav picture of what you are doing with it so that they can make informed cho

There is no doubt that complying as this can be onerous, but it is important to keep in mind that there at make it worth the effort. Not least is the fact that by providing the rec n, you reduce the risks associated with non-compliance, which can inc

A small business might well consid e Information Commissioner's list of priorities, but by showing a willingn out your use of personal data, you may benefit from improved levels o prove your business' reputation but may even mean that individuals ar e useful personal information about themselves.

Part 3. Exceptions

As important as the right to be infor limited exceptions. You are not, for example, required to provide data tion that they already have when collecting personal data from them.

If you collect personal data from thi ed to provide privacy information to the data subjects whose data is invo

- They already have the requi
- It would be impossible to pro ion;
- It would involve disproportion privacy information;
- Providing the privacy infor impair (or make impossible) the achievement of the objective ocessing;
- Obtaining or disclosing the p is a legal requirement; or
- You are subject to an obliga ecy regulated by law that covers the personal data in question.

It is important to note that the secon apply in particular to processing for archiving purposes in the public int cal research purposes or statistical purposes, subject to the conditions et out in Article 89 of the UK GDPR (as supplemented by section 19 of t 2018). This suggests, therefore, that SMEs using personal data for bu struggle to justify relying on the exceptions.

Furthermore, whatever your justifica xception, it is important to document your decision-making process and case with all decision-making and management relating to data protec

Even if an exception could apply, e your Privacy Information publicly available, so as to increase the cha ubjects will see it. As a general rule, however, particularly in the SME uld suggest that providing Privacy Information directly as a matter of c d choice.

Part 4. Drafting Privacy Inf ge

As noted above, it is important th nformation in a concise and user-friendly way. An important part of our audience. Privacy Information presented on a business-to-busine nal services may, for example, be presented in a more technical man onsumer website offering goods or, an example requiring even further t ted at young people. In any case, it is good practice to avoid technical a as possible.

The Information Commissioner's C g your Privacy Information out on your target audience, amending it a user feedback.

You should also ensure that you reg y Information to ensure that it is up-to-date with your actual use of per e latest changes in the law, official guidance, and best practice.

Part 5. Dealing with Chang

The ways in which a business us e relatively fixed or relatively fluid, depending upon the nature of the b which new projects are handled. As covered in detail in our other Guidar ction Impact Assessments and Data Protection Audits, it is important tha al data are properly managed.

If a new use of personal data is co nal lawful basis for processing, you may be able to continue with the further action, unless your original basis was consent. If, on the othe personal data is different from the original use, you must identify and d asis for processing it.

Consequently, your Privacy Informa ged to ensure that data subjects are kept fully informed of the ways in w their personal data. If any changes are made, it is important that you the attention of the affected data subjects.

Part 6. Dealing with Other

It is quite common for one organisa ta to involve other organisations. In some cases, these third parties will data in some way or another under the instructions of your business. In rty will be a data processor. In other cases, personal data may be share , with the recipient left to determine what they will and will not do wit at the data will have been shared between two controllers.

Regardless of the context, the sha ill have an impact on your Privacy Information. As stated above, if you m third parties rather than from the data subjects to whom the data rela ning of your provision of the Privacy Information as well as its content. S rsonal data that you have collected with others, you must tell the data s the names of the organisations you are sharing their data with or at leas e organisations fall under.

Sharing Personal Data with Other

It is important that data subjects kn are sharing their personal data with, irrespective of whether the recipient acting as a data controller or a data processor.

The UK GDPR requires you to iden personal data or, at the very least, the categories of recipient. It may e, that a contractor with whom you share customer information for pro ommercial reasons for keeping the identities of their clients confidentia could simply identify them by their category (e.g. IT service provider) r m directly. What matters is that the information given to data subjects s them a clear picture of what is happening with their personal data.

Wherever possible, individual data n a choice. This will not always be practical, but wherever it is, a choice ercise that choice should be given.

Obtaining Personal Data from Oth

If you obtain personal data, for exa third party, you are still required to provide Privacy Information to the c nless you are able to rely on one of the exemptions outlined above in ady observed, however, we would consider it less likely that one of the ly to the typical small business.

If an exemption does apply and you g Privacy Information would involve disproportionate effort or would be required to find ways of mitigating risks associated with processing t ed. Conducting a Data Protection Impact Assessment is the best way

As explained in Part 5, above, you ta subjects are made aware of any change in purpose and the lawful b ing in cases where personal data is being used for a purpose different t ginally collected.

As also noted above, while you a de Privacy Information at the time personal data is collected in this w urse), you are required to provide it within a reasonable period of obtai ter than one month (or, if earlier, if you communicate with the data su nsfer the personal data to another party).

Obtaining Personal Data from Pu s

Even if personal data is drawn from s, it is not a free-for-all. The Privacy Information requirements continue t tion applies (as above).

As when obtaining personal data s must be mitigated, and a Data Protection Impact Assessment con at it is impossible or would involve disproportionate effort to provide Pri

Even though personal data may be idual data subjects still need to be kept informed and their personal suse. If your plan is to use their personal data in a way that might b ve (the Information Commissioner's Office gives combining data from example), it is important that clear information about that processing is

As above, Privacy Information must sonable time, and no later than one month after obtaining the personal d r, as appropriate).

Part 7. Artificial Intelligenc cision-Making

AI and machine learning are as ing now as the venerable phrase "making the world a better place", b yreal and increasingly applied in the business world. While at this stage, assume that most small businesses will not be using AI, the increasing a logy tools could make it a reality for many sooner rather than later.

AI can take many forms and in bus ul for automated decision-making – something that the UK GDPR has places. If such automated decision-making has 'legal or similarly signi rtant that your Privacy Information explains what personal data will be s relevant, and what the impact will likely be on the data subjects conce

In some cases, as new technologies existing personal data – a customer database, for example – will be us ose new technologies. It is always important to remember that, as stat u are using personal data for a new purpose, individual data subjects m ou start and, if necessary, you must obtain fresh consent for the new pu ur basis for using the personal data originally).

Part 8. Conclusions

At the core of the UK's data protect incipally of the UK GDPR and Data Protection Act 2018 are the princip ss, and transparency. These three principles are inextricably linked, nc ut also to the rights bestowed upon individual data subjects.

Personal data can be an extrem asset. In many cases, day-to-day business functions could not take p asingly it has further value. The law recognises and supports this valu alance it by protecting individuals' interests and ensuring that organisa ir personal data, fairly and openly.

Providing comprehensive and user tion is a key ingredient in the data protection mix. It may, at times, be have the unfortunate by-product of highlighting personal data use that tomers would object to. Ultimately, however, the benefits of complying ht to be informed, should outweigh the costs. Not only is your own posit reduced your exposure to penalties for non-compliance with the law, but omer base goes a long way.