Privacy Notice

Retail Manager Solutions Limited (RMS)

1. Introduction

1.1 RMS takes your privacy seriously and is committed to compliance with the GDPR and Data Protection laws. In this Privacy Notice you can find out about your privacy rights and how we collect, use, share and secure your personal identifiable information (personal information). This includes the personal identifiable information we already hold about you now and the further personal identifiable information we might collect about you, either from you or from a third party.

1.2 This Notice sets out our commitments to you and our clients to whom we process personal information on their behalf and under their instructions to be compliant with the Data Protection Laws in the countries in which we operate. It explains how we collect, use, store, share and secure your personal information and how we comply based on our relationships and processing operations with individual's personal information in delivering our products and services.

1.3 This Privacy Notice is a public document available when RMS obtain and use your personal identifiable information. It explains how we as a **data controller** for our own recruitment, employee, accounting and marketing purposes and how we as an appointed **data processor** for our clients provide software solutions to enable them to process and manage their services and the personal information regarding individuals contained within these solutions will be managed in line with the Data Protection Laws. In both circumstances we obtain and process individual's personal identifiable information in order to conduct our normal business operations and to deliver products and services to our current and prospective clients.

1.4 The difference between a **data controller** and **data processor** is important. You have certain rights in relation to your personal information, for example the right to be provided with the personal information held about you and details of its use and the right to have certain of your personal information either erased or anonymised, commonly referred to as the right to be

forgotten (see below to see what rights you have). These rights can only be exercised against a data controller of your information. We will be a:

- **Data controller** of our own applicants, employees and individuals to whom we carry out direct marketing operations.
- **Data processor** for a data controller (our clients), holding and processing your personal information under their instructions.

1.5 RMS operating as a data processor: we would only act on the instructions of our clients as data controllers when you exercise your rights. When informed we will co-operate fully and in a timely manner to ensure our clients as data controllers can respond to you in line with the Data Protection Laws in the UK and under the General Data Protection Regulation, (GDPR). Our client as the data controller will supply you with a privacy notice at the first point of contact with you and as part of this they will inform you we are one of their third-party suppliers and as such we act as a data processor.

1.6 RMS operating as a data controller: we will make the determination on how we will obtain, use, store, share and secure your personal information either as an applicant as part of our recruitment process, employee, visitor to our website and/or as part of our marketing operations with individuals and with our current and prospective business clients. As a data controller we will supply you with a privacy notice at the first point of contact with you. This notice constitutes our privacy notice and provides you with details on how we will process your personal information.

1.7 As a data controller we will only provide this privacy notice to you once, generally at the start of our relationship with you. However, if the applicable privacy notice is updated substantially, then we may provide you with details of the updated version. You are encouraged to check regularly for updates.

1.8 As we hold and process a volume of individual's personal information and special categories of information for our clients (data controllers) as part of our core activities, we have appointed a voluntary Data Protection Officer (DPO), whose details are below and you can contact them if you have questions about your data, data protection, your rights or make a complaint:

By post:	By email:	By phone:
Information Rights Manager	DP@retail-manager.com	02380 816000
Retail Manager Solutions Limited		
Castle Malwood		
Minstead		
Hampshire		
SO43 7PE		

2. Who we are

2.1 Where we refer to 'we' or 'us' in this Privacy Notice, we are referring to RMS responsible for the collection, processing, storage and safe keeping of any personal and special categories of information you provide us with as part of your relationship with us. Where we are a data controller the information you provide will be managed in accordance with the Data Protection Act 2018 and General Data Protection Regulation (GDPR). We are registered as Data Controller with the Information Commissioners Office under the registration number: Z1708844

2.2 RMS provides and sells products and services in the form of software solutions to our clients where we process personal information relating to their customers (data subjects). Therefore, as a data processor for our clients we have entered into contractual obligations in regards to data protection. The products and services we provide are:

- Unified Comms from version 1.0;
- Operations Director and People from version 4.0;

We also host our client's information in a secure manner in compliance with the law.

3. Your privacy rights

3.1 From the 25 May 2018 you have eight rights relating to the use and storage of your personal identifiable information. A Data Controller must comply with these rights and they are:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

For further information as to your rights, please refer to Appendix A to this Notice – Individual's Rights Explained

3.2 In brief, you have the right to be informed who is obtaining and using your personal identifiable information, how this information will be retained, shared and secured and what lawful grounds will be used to obtain and use your personal identifiable information. You can view the lawful grounds we will rely on as a Data Controller at Appendix B to this Notice - Lawful Basis Processing. You have the right to object to how we use your personal identifiable information in certain circumstances. You also have the right to obtain a copy of the personal identifiable information we hold about you.

3.3 In addition, you can ask RMS to correct inaccuracies, delete or restrict personal identifiable information or to ask for some of your personal identifiable information to be provided to someone else. You can make a complaint if you feel RMS is using your personal identifiable information unlawfully and/or holding inaccurate, inadequate or irrelevant personal identifiable information which if used may have a detrimental impact on you and/or has an impact on your rights.

3.4 You can also make a complaint to the data protection supervisory authority. In the UK, this is the Information Commissioner's Office, at https://ico.org.uk. You can view other supervisory authorities and details of countries where your personal identifiable information is held and processed by RMS here:

Microsoft (infrastructure/software):
https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx
AWS (infrastructure): https://aws.amazon.com/compliance/gdpr-center/
Twilio (discussion/conferencing): https://www.twilio.com/gdpr

SendGrid (mailing service): https://sendgrid.com/policies/tos/

3.5 To make enquires for further information about exercising any of your rights in this Privacy Notice, please contact our DPO, the details for which are as stated above.

4. What Kinds of Personal Identifiable Information do we use?

4.1 We use a variety of personal identifiable information depending on the services we deliver to you. For all services, we may need to use the following information about you:

Personal Information

- Contact details - name, address, email, home and mobile telephone numbers;
- Age – date of birth;
- Identification - information to allow us to check your identity;
- Photograph – information to record your identity;
- Online computer identification (IP address) – information recorded when you engage with us by email;
- National Insurance numbers – information to carry out functions such as payroll and/or supporting people contracts;
- Next of kin
- Marital Status
- Occupation
- Reference Numbers (e.g. passport) where your personal information appears

There are other types of personal information which we collect for the purposes of our relationship with you either as you have engaged with our products or services or that of our clients. The personal information we hold are:

Special Information

- Health - to support our Health and Safety operations in the work place;
- Race – optional, and solely to support our equality monitoring purposes;
- Ethnic origin – optional, and solely to support our equality monitoring purposes;

There are other types of special information which we do not collect but are deemed important under the law:

- trade union membership;
- biometrics (where used for ID purposes).

We also act as a data processor with our clients where we have entered into a contract to deliver software services and platforms which hold individuals personal and special information. It will be the responsibility of our clients, as the Data Controllers, to issue a privacy notice and we will co-operate in the process outlined in such notice.

4.4 Sometimes where we ask for your personal identifiable information to enter into a contract/agreement with you, for example in relation to our relationship with you in the performance of a contract with you or as we have a legal or regulatory duty. It could be a simple process of attaching a cookie to enable a transaction to take place. We will not be able to provide some of our services or products without this information.

4.5 We collect and use your information as part of our recruitment process and we would be required, where the role requires, to collect and process your personal and special information when you submit an application or CV to work for RMS. We will use your personal information for the purpose of the application process and to produce and monitor recruitment statistics. Your personal information as detailed in 4.1 will be used in regards to your employment within RMS to carry out work duties and for purposes of payroll.

5. How We Gather Your Personal Identifiable Information

5.1 We obtain personal identifiable information by various means; this can be by an application form, face to face, email, telephone, correspondence and/or by receiving this information from others, for example: an authorised person representing you, police, health or social care agencies. We can also receive information about you from other people who know you and/or are linked to you, for example: nominated person to act on your behalf, a nominated 'Responsible' person for a child or your legal representative.

5.2 Some further examples of how we may gather your personal identifiable information are set out below:

- directly from you, for example: when you fill out our application form for a job;
- from monitoring or recording calls as part of quality and complaints monitoring: we record these calls for training and to ensure the safety of our staff;
- from monitoring your use of our website; and
- from information shared by your previous employer with your consent.

6. How We Lawfully Use Your Personal Information

6.1 When you apply to work for RMS, we will need to obtain your name, contact details, date of birth, your current and previous countries of residence/citizenship, and a copy of identification documents (such as passport, home office residence papers and driving license) where we are required to for the right to work in the country.

6.2 We will from time to time share information with third party suppliers (data processors) to carry out functions on our behalf, for example to a payroll company to deliver you your salary each month. When sharing your information, we will have applicable contractual clauses applied where all of these recipients will demonstrate compliance with data protection laws and your rights.

6.3 There are some cases when we will share your information where it is necessary for legitimate business purposes. This will be to ensure that your needs are met and to also meet the health and safety obligations we have as an employer when delivering a service. This may include sharing information with other partnering organisations and our contractors and partners:

- In order to carry out our contractual obligations; and
- So that third parties can carry out our duties/functions/events on our behalf

You can see the categories of third party contractors and sub-contractors we use here:
Microsoft (infrastructure/software): https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx
AWS (infrastructure): https://aws.amazon.com/compliance/gdpr-center/
Twilio (discussion/conferencing): https://www.twilio.com/gdpr
SendGrid (mailing service): https://sendgrid.com/policies/tos/
Staff Payroll: https://www.star-payroll.com/

7. Automated decision making

7.1 We do not carry out any automated decision making as part of our processing operations as a data controller. When delivering software services as a product this processing may take place and it will be our client who is the data controller to inform individuals of the processing operations and individuals rights.

8. Our Legal Basis For Using Your Personal Identifiable Information

8.1 We only use your personal identifiable information where that is permitted by the laws that protect your privacy rights. This will be where:

- we need to use the information to perform a contract or enter into a contract with you;
- we need to use the information to comply with our legal obligations;
- we need to use the information for our data controllers legitimate interests

When we consider using your information for the last purpose stated above we will consider if it is fair to use the personal identifiable information either in our interests or someone else's interests, and only where there is no disadvantage to you – this can include where it is in our interests to contact you about like for like products or services from RMS to a business and RMS to a person. Where we carry out direct marketing operations with businesses we will carry out a marketing assessment to market to you or collaborate with others to improve our services. Where we need to seek your consent, we will (if consent is needed).

8.2 Where we have your consent, you have the right to withdraw it. We will let you know how to do that at the time we gather your consent. See section 12 Keeping You Up to Date, paragraph 12.1 for details about how to withdraw your consent to marketing.

8.3 Special protection is given to certain kinds of personal information that is particularly sensitive. This is information about your health status, racial or ethnic origin, political views, religious or similar beliefs, sex life or sexual orientation, genetic or biometric identifiers, trade union membership. We will only use this kind of personal information where:

- we have a legal obligation to do so (for example to protect vulnerable people);
- it is necessary for us to do so to protect your vital interests (for example if you have a severe and immediate medical need whilst on our premises);

- it is in the substantial public interest;
- it is necessary for the prevention or detection of crime;
- it is necessary for insurance purposes; or
- you have specifically given us 'affirmative' consent to use the information.

9. Sharing Your Personal Information or Getting Your Personal Identifiable Information from Others

9.1 Our clients in the use of our software products may supply personal identifiable information or special information. We receive this as we are a data processor and we shall follow the instructions of our clients as data controllers in the hosting of this information and the security to which the information will be retained under.

10. Transfers outside the UK

10.1 We may need to transfer your information outside the UK to Australia (where RMS have a branch office) and to service providers, agents, subcontractors and regulatory authorities in countries where data protection laws may not provide the same level of protection as those in the European Economic Area. When transferring data we will ensure that your personal information is only used in accordance with this privacy notice and applicable data protection laws and is respected and kept secure and where a third party processes your data on our behalf we will put in place appropriate safeguards as required under data protection laws.

10.2 Our directors and other individuals working for RMS may, in limited circumstances, access personal information outside of the UK and European Union, e.g. if they are on holiday or working abroad outside of the UK or European Union. If they do so they will be using our security measures and will be subject to their arrangements with us which are subject to English Law, in line with the GDPR and the same legal protections that would apply to accessing personal data within the UK.

10.3 Where we transfer your data outside of the UK, the RMS Solutions and environments will provide for the best security and availability practices including dual data-centre usage as a minimum to ensure constant availability of access to data; Firewalling controls; Anti-Virus/Malware services; IPS/IDS servicing; 24-hour systems' monitoring and alerting

functions; obfuscation/encryption of any sensitive data; encryption of all traffic between systems, including to the client's system; encryption at rest; authentication options for password controls and complexity; authorisation levels with no access by default and least required level access provision. In addition, RMS support personnel follow security training, policies and procedures, and additionally will not have direct access to view or extract client sensitive data direct from data sources.

11. How Long We Keep Your Personal Information For?

11.1 How long we keep your personal information for depends on the services we deliver to you. We will never retain your personal identifiable information for any longer than is necessary for the purposes for which we need to use it.

12 Keeping You Up To Date

12.1 We will communicate with you about products and services we are delivering using any contact details you have given us - for example by post, email, text message, social media, and notifications on our 'App' or website. Where you have given us consent to receive marketing, you can withdraw consent, and update your marketing preferences by contacting us directly contact@retail-manager.com. Visit our website at www.retail-manager.com.

13. Your online activities

13.1 We use cookies, which are small data files which are placed on your computer or other device by our website, and which collect certain personal data about you. This enables us to tailor our product and service offering (including our website) to provide you with products and services which are more relevant to your company's requirements, if you have given consent.

13.2 RMS may also collect information about usage of this website. We use this information either to respond to a specific request or to help us understand how the website is used. We may analyse information collected to help develop our business and improve the services we provide. We may also use this information to contact you for opinions on our services or to notify you from time to time about changes to our business or updates to the website.

13.3 You may change your website browser settings to reject cookies, although please note that if you do this it may impair the functionality of our website or of other websites.

14. Confidentiality and security

14.1 We have implemented security policies, rules and technical measures to protect individual's personal information that we have under our controlfrom:

- Unauthorised access
- Improper use or disclosure
- Unauthorised modification
- Unlawful destruction or accidental loss

14.2 All our employees, representatives, board members and third-party contractors (data processors) which we engage, who have access to, and are associated with the processing of your personal information, are obliged to respect the confidentiality and only process the information based on our instructions. We ensure that your personal information will not be disclosed until all security assurances have been documents.

15. RMS Commercial and Employee Information

15.1 When someone visits our website we will collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site. We collect this information in a way which does at times identify a person who contacts us about a product. We do not make any attempt to find out the identities of those visiting our websites as a routine search. If we do want to collect personally identifiable information through our website, we will be up front about this. We will make it clear when we collect personal information and will explain what we intend to do with it.

15.2 Except as set out in this privacy statement, we will not disclose, sell or rent your personal data to any third party. If you do consent but later change your mind, you may contact us and we will cease any such activity. In the event that a third party acquires all or part of our business and/or assets, we may disclose your personal data to that third party in connection with the acquisition, but only where lawful and compliant with the Data Protection Act 2018 and General Data Protection Regulation (GDPR) and the relevant UK data protection

legislation. We may also disclose your personal data where necessary to comply with applicable law or an order of a governmental or law enforcement body.

APPENDIX A

YOU'RE RIGHTS IN RELATION TO YOUR PERSONAL INFORMATION

In responding to your rights, we will need to obtain the following information:

1. Proof of your identification
2. Enough information from you to locate the information

A. The **right to be informed** about how your personal information is being used:

We shall supply and keep updated our privacy notices to you as a visitor to our website, current or former employee and/or an applicant applying for a job with RMS. We shall detail:

1. Who we are
2. What information we collect, use, share, store and how long we will retain your information
3. The lawful grounds we have applied to process your information and when we need consent
4. How we will keep your information secure
5. How we will keep your information safe when we transfer it outside the UK
6. The likely recipients to whom we may share your information with
7. How you can exercise your rights and object to processing
8. The source of the information
9. How to make a complaint to us as the Data Controller and the Supervisory Authority (Information Commissioner's Office)

B. The **right to access** the personal information we hold about you:

We will need to obtain the following information when processing your request for a copy of your personal information:

1. **Proof of your identification**
2. **Enough information from you to locate the information**
3. **Authority to act form if you have engaged a representative to act on your behalf**

Once point 1 and 2 are completed we have one month to respond with a copy of your information by electronic or paper-based means whichever is applicable in the circumstances. There is no charge, but we may as detailed under the law:

a) Refuse a request if it is deemed manifestly unfounded or excessive
b) Refused a repeat request for information again based on the above point, however if the information has changed since our last request and enough time has passed we will process the request based on point 1 and 2 above.

For RMS customers, a Subject Access Request (SAR) can be raised on the RMS support system by the customer's/client authorised personnel, for actioning by RMS.

C. The right to request the **correction of inaccurate** personal information we hold about you:

It is important you keep us informed of any changes regarding your information which you have supplied us. You have the right to request your information to be rectified if it inaccurate or incomplete or you can ask us to add more details to the information to make it correct. To activate this right you need to:

1. Detail clearly what you believe to be inaccurate or incomplete
2. Explain how you would like us to correct this information

3. Supply evidence of the inaccuracies

The request can be received by telephone, (verbal); however, we recommend you follow this in writing as it allows you the opportunity to explain and give examples/evidence why your information is inaccurate or incomplete and what your desired outcome is. For RMS customers, a Subject Access Rectification (SARE) can be raised on the RMS support system by the customer's/client authorised personnel, for actioning by RMS

Once we receive your request we will:

a) Review the request and carry out an assessment of the information
b) If the information is inaccurate or incomplete we will make the necessary changes (e.g. corrected, deleted or added information). We will contact you via our support process in writing within once month of receiving your request confirming our actions, or

D. The **right to request erasure** of your personal information:

You can contact us to request the deletion of your information in certain circumstances; if you want to have your information erased you need to detail clearly what you want erased.

The request can be received by telephone (verbal), which should be followed up in writing as it allows you the opportunity to explain and give examples what information we hold which you want erased. For RMS customers, a Subject Access Erasure (SAE) can be raised on the RMS support system by the customer's authorised personnel, for actioning by RMS.

Once we received your request we will:

a) Review your request and if the information is not required for one of the purposes detailed in point c, we will erase the information.
b) Where your information which we have agreed to erase is held on public online environment (e.g. social networks, forums, websites) which we have posted, then we will take reasonable steps to inform these 'Information Societies' about the erasure and request the remove this. This is called the 'Right to be Forgotten'.
c) When we carry out this process we will contact any likely recipients which may hold this information and request them to erase the information. We shall keep a record of this request and our action. In the circumstances where we do not agree to erase your information, we will detail in writing the reasons why. These could be based on the reasons above and/or as the information falls into the criteria of the freedom of expression and that includes journalism, academic, artistic and literary purposes. Where there is a requirement to retain information is needed to be retained for public health reasons or the information is necessary for establishing or exercising / defending legal claims. In limited circumstances it could be refused on the basis of prejudice, scientific or historical research or archiving that is in the public interest. We may refuse the request if it is deemed manifestly unfounded or excessive.

E. The right to **restrict processing** of your personal information:

You can contact and ask us to stop processing your information if you are concerned about the accuracy of the information we hold and use. In certain circumstances you can also ask us not to delete your information from our records. This right is closely linked with the right of accuracy and the right to object. You can ask us to temporarily limit the use of the information if your disputing our decision on the accuracy of your information or an objection on how we use your information. You can also ask us to limit the use of the information rather than delete it if you feel we have unlawfully used your information we no longer need the information but you want us to keep it in order to create, exercise or defend a legal claim. If you want to have your information restricted you need to detail clearly what information you want us to stop processing.

Once we receive your request we will:

a) Consider the request and take appropriate steps to restrict the use of your information as we agree with your objection. We could temporarily move your information to another system, make it unavailable to users, or remove it from a website, if it has been published in the public domain. Where we have shared the information, which is restricted with recipients where it is proportionate to do so, we will contact them asking them to restrict the information in question. We will hold the restricted data securely and shall not use it further unless:
    i) we have your consent,
    ii) it is needed for legal claims,
    iii) to protect a person's rights, or
    iv) it is in the public interest.
b) If we have applied restrictions on the information during our assessment once this is concluded, we may lift the restriction. We shall inform you in writing of this decision.

The request can be received by telephone, (verbal); however we recommend you follow this in writing as it allows you the opportunity to explain and give examples what information we hold which you want us to stop processing.

If we do not agree with your request to restrict your information we will contact, you in writing within one month of receiving your request confirming the reasons why. If the restriction impacts on our duty to carry out our duties under a contract with you or our legal or regulatory obligations, we may not be able to agree with your request.

F. The right to **object** to the processing of your personal information:

You can object to your information being used for direct marketing , this is an absolute right and one which we feel strongly about, we will only market businesses and/or people if they have consented and/or we are delivering like for like products and services which you have previously engaged to receive. You can object at any time and withdraw your consent free of charge - click here to unsubscribe: Unsubscribe. You can ask us some questions to help you decide if you want to object to how we use your information, this is because you ***can only object*** to the use of your information when we are using it for:

- To carry out a task in the public interest
- For our legitimate interests
- Scientific or historical research, or statistical purposes, or
- Direct marketing.

The above four areas are the only areas you have a right to object to. If you want to object to how we use your information is used the above circumstances you need to:

1. Detail clearly what to object to and why we should stop processing this information.
2. If you want to object to direct marketing you can simply unsubscribe by clicking here: Unsubscribe.

Once we receive your request we will:

a) Consider the request and take appropriate steps to assess your objection and where the grounds are established and agreed upon we will stop using your information.
b) Where we have shared the information with recipients and where it is proportionate we will contact them asking them stop using your information.

The request can be received by telephone, (verbal); however, we recommend you follow this in writing as it allows you the opportunity to explain and give examples what information we hold which you want us to stop processing.

If we do not agree with your objection we will contact, you in writing within one month of receiving your request confirming the reasons why. The type of circumstances where we may not agree with your objection are:

- When we deem the request to be manifestly unfounded or excessive;
- If your request is repetitive; or
- If the objection impacts on our duty to carry out our duties under a contract with you or our legal or regulatory obligations.

However, we will note your objection and supply you details of how to complain to the Supervisory Authority (Information Commissioner's Office).

G. The right to request that we transfer elements of your data "**Portability**"

You can request us in certain limited circumstances to transfer elements of your information to another organisation in a way that is accessible and machine-readable, for example by supply sets of your information in an excel form. This right only applies to information held electronically, and where you have provided the information. This does not apply to information you have typed in for example your username and email address. Its focus is on the type of information we have gathered from our monitoring activities on how you have used a devise or service on a website, search usage history, traffic and location of information. You can make a portability request when we rely:

- On your consent to use your information
- As part of a contract with have with you

If you want to request your data to be transferred, you need to detail precisely what information you require to be transferred.

Once we receive your request we will:

a) Consider the request and take appropriate steps to assess your request.

The request can be received by telephone, (verbal) but should be followed up in writing as it allows you the opportunity to explain and give examples what information you want transferred and to whom. For RMS customers, a Subject Access Portability (SAP) can be raised on the RMS support system by the customer's authorised personnel, for actioning by RMS

If we do not agree with your request we will contact you in writing within one month of receiving your request confirming the reasons why. The type of circumstance's where we may not agree with your objection are:

- When we deem the request to be manifestly unfounded or excessive
- If your request is repetitive
- If the objection impacts on our duty to carry out our duties under a contract with you or our legal or regulatory obligations we may not be able to agree with your request.

H. The right to **object to certain automated decision making**:

When decisions are made about you without people being involved, this is referred to as 'automated decision making'. You have the right to prevent automated processing when it falls into the following two grounds:

- Automated individual decision-making
- Profiling

This could be when we have carried out an aptitude test using a pre-programmed algorithms and criteria and/or where we have had to carry out a credit reference check as part of our contract and anti-money laundering purposes when we enter into a contract with a client / person. Profiling could relate to processing information for the performance at work, economic situation, health or personal preferences

and interests. It could also relate to our marketing operations and these processes can be carried out by electronic means, internet searches, social networks, mobile phones or lifestyle information.

We will only make decisions solely on automated processing if the decision affects a person's legal rights if it is necessary for the purposes of a contract, or to meet a legal obligation and where we have your consent. We will always inform you why a decision was made and the manner in which it was reached.

Once we receive your request we will consider the request and take appropriate steps to assess your request and reach a decision.

The request can be received by telephone, (verbal); however, we recommend you follow this in writing as it allows you the opportunity to explain and give examples what information you want transferred and to whom.

If we do not agree with your request, we will contact you in writing within one month of receiving your request confirming the reasons why. The type of circumstances where we may not agree with your objection are:

- When we deem the request to be manifestly unfounded or excessive
- If your request is repetitive
- If the objection impacts on our duty to carry out our duties under a contract with you or our legal or regulatory obligations, we may not be able to agree with your request.

Our Response to you

Normally we will respond to you within one month of receiving your request.

As a data controller the law permits us to extend the time to supply the information requested from one month to three months from the date your request is deemed valid. We will only consider extending the period in which we must respond if your request is complex or you make more than one request.

If the request is deemed to be manifestly unfounded or excessive, we have a right to charge a fee according to the law, and the fee will be based on administration charges only, (cost to prepare, respond and provide written evidence of our decision).

If we do not agree with your request in relation to any of the above, we will contact you in writing within one month of receiving your request confirming:

- We have acted on your requests and have processed the request in line with your rights and the law; and
- The reasons why we have refused your request and the basis we have relied on.

If you are unhappy with our decision you can raise a complaint with the Supervisory Authority (Information Commissioner's Office).

APPENDIX B

GDPR Lawful Basis Processing

Under the General Data Protection Regulation (GDPR) there are 6 lawful bases in which a data controller can process the personal data of data subjects (customers, staff, contractors, etc.). A data controller should firstly establish grounds to process data under grounds 2 to 5 for personal and if processing special categories of data (e.g. sexuality, religion) then a further ground set down in Article 9. Under Article 6 the lawful grounds are:

1. **Consent:**

   The differences for consent between the Data Protection Act 1998, definition:

   "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*"

   The GDPR's definition:

   "*any freely given, specific, informed and **unambiguous** indication of the data subject's wishes by which he or she, **by a statement or by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her*"

   There is a higher bar for consent with the GDPR, the idea is that the data subject is fully aware of what they are potentially signing up for and is given a choice as to accept or refuse to give their consent. If they have given their consent they need to be able to withdraw the consent at any time and you need to inform them how, with no cost to them.

   The data subject has to be aware exactly what they are signing up to, in a clear and concise format and if the service is being directed at children it needs to be in a format that the child can understand. These notices can either be in written or verbal, such as a video.

   The data controller needs to have mechanisms in place to record when consent has been obtained as well as when it has been withdrawn and their systems need to ensure that only the data subjects who have given consent are contacted and once they withdraw the system needs to ensure they are not contacted.

2. **Contract:**

   There needs to be a supply of goods or services that have been requested by the individual or to fulfil obligations under an employment contract. This also applies to any steps necessary to enter into the contract, e.g. the application stages before employment.

   While this will normally be the basis of why data is being collected it is still worth looking over what information is collected at the various stages of the process, splitting up the processes and going through each field on an application form and asking the question why is this data necessary? If the data controller cannot justify why they are collecting, then it maybe that the data is not necessary and maybe excessive and therefore may not be required.

   It could when looking through the different stages of a process that the data controller may move some of the collection carried out to a later stage in the process e.g. asking all applicants for a job to provide details of their qualifications and taking copies of passports. It maybe that

just ensuring a record that these items have been seen would be sufficient rather than holding data for all applicants when you are only going to appoint one person. The data could be asked for again during the notice period or when contracts are signed.

3. **Legal obligation:**

   This is where the data controller is processing data as it is required by law either in the UK or EU to process the data, this does not include any contractual obligations.

4. **Vital interests:**

   The data controller can process personal data if by doing so protects someone's life. This can be either the data subject or someone else.

5. **A public task:**

   If the data controller is processing data which is in the public interest – and they have a legal basis for processing the data under UK law then this is lawful. It is deemed that any public body, Local Authority, National Health, any company governed under the Freedom of Information could use this legal basis for most if not all of their processing.

6. **Legitimate interest:**

   If the data controller is a private sector organisation, they will be able to process the data without the consent of the data subject if they have a genuine and legitimate reason, which also includes any commercial benefit. This would not be the case if there was potential to harm the data subject's rights or interests.

   Data controllers can consider this basis where consent would deem to be inappropriate or is seen to be manifestly unfounded. The data controller can continue to process their data even without the consent of the data subject/s. The data controller would still need to ensure there is no unwarranted impact on the data subjects and that the processing is still under the principles fair, transparent and accountable.

Special Categories of Data:

As with the present law, the Data Protection Act 2018, to process sensitive data, under the GDPR this is now known as ***Special Categories of Data***, the data controller still needs to satisfy a lawful basis for collecting personal data, Article 6 of the GDPR, these are listed above 1-6, and will need to satisfy a further condition to process this type of data, Article 9.
This is because special category data is more sensitive, and so needs more protection. For example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

The conditions for processing special category data are listed in Article 9(2) of the GDPR:

(a) the data subject has given ***explicit consent*** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the ***obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection*** law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) processing is necessary to ***protect the vital interests*** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its ***legitimate activities*** with ***appropriate safeguards*** by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly ***made public by the data subject***;
(f) processing is ***necessary for the establishment, exercise or defense of legal claims*** or whenever courts are acting in their judicial capacity;
(g) processing is necessary for ***reasons of substantial public interest***, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the ***purposes of preventive or occupational medicine***, for the ***assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care*** systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
(i) processing is necessary for reasons of ***public interest in the area of public health***, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
(j) processing is necessary for a***rchiving purposes in the public interest, scientific or historical research*** purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Processing children's data

Under the GDPR any data controller who is using social information services (e.g. Facebook, media etc.) and their target audience are children, under the age of 13 in the UK Data Protection Act 2018, will need to verify the age of the child and will need parental consent if the child is under 13. The data controller needs to verify the person giving consent of behalf of a child has the legal right to do so, by using available technology.

Any notices need to be made age appropriate when engaging children so that they are clear on what the data controller is offering and what they are consenting to.

There are exceptions although they are limited when dealing with children's data and they will normally be around safeguarding the child, for example consent would not be asked if there was a concern of abuse within the home, either from the child or the parent/guardian.

The Organisation may be holding a fun day and employ a photographer who will need to present anyone they are photographing a consent form if the photograph puts that person as the focus (e.g. they are the only one in the photograph). If the image is a ‘wide public shot’ then there is no expectation of privacy.

There is no age limit for such activities however if they are relying on consent then the data subject will need to understand the form they are signing and it up to the data controller to ensure this is the case. The data controller will also need to ensure that the person who is offering to sign a consent notice on behalf of a child has a legal right to do so.