Subject Access Request Policy and Procedure

Frost Group Limited

Subject Access Request Policy and Procedure

CONTENTS

Purpose

The purpose of this document is threefold:-

1. To provide data subjects with a framework within which they can request personal data held by either Frost Group Limited or an insolvent entity under the control of insolvency practitioners taking formal appointments for Frost Group Limited.

2. To assist both external and internal data subjects (i.e. staff) in obtaining personal data to which they are entitled both under the Data Protection Act 2018.

3. To provide the Compliance Officer and Board of Frost Group Limited with a framework within which to manage the provision of personal data in response to Subject Access Requests ("SAR").

1. Our Best Practice

1.1 Frost Group Limited has high standards which all individual members of staff are required to endeavour to achieve both as individuals and as a team.

1.2 This document is part of a set of manuals, policies and procedures in which we have set out the standards that are required and how to achieve them.

1.3 All staff have a personal responsibility to ensure they are aware of these standards and how we aim to achieve them.

2. Subject Access Request

2.1 All private individuals who believe that personal data is held by a third party have a right to make a Subject Access Request under the Data Protection Act 2018 ("DPA18") which enacted the General Data Protection Regulations ("GDPR") issued by the European Union on 25 May 2018. DPA18 enables a private individual to obtain copies of the personal data held on them by Data Controllers and Data Processors and to exercise their statutory rights over that data.

2.2 DPA18 applies to personal data, including human resources records, customer lists, contact details etc. DPA18 apply to data contained both on automated and manual records. DPA18 extend to sensitive personal data including genetic/biometric data which can be used to uniquely identify a person.

2.3 It is necessary to obtain the explicit consent of the data subject to hold data, as such businesses can no longer rely on opt out boxes to retain data as there must be a positive opt in. Consent must be given freely, be specific, informed and an unambiguous indication of the individual's wishes. Privacy notices must be clear enough for children to understand and consent must be obtained from a parent or guardian subject to the age of the child concerned and the prevailing member state law.

2.4 Data held must be necessary for the performance of a contract with the data subject or to take steps to enter into a contract with the data subject.

2.5 Processing must be necessary for the performance for compliance with legal obligations.

2.6 Processing is necessary to protect the vital interests of a data subject or another person.

2.7 Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

2.8 Processing is necessary for the purposes of legitimate interests pursued by the controller or third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

2.9 Explicit consent is required unless reliance on consent is prohibited by EU or member state law.

2.10 Processing is necessary for the carrying out obligations under employment, social security or social protection law or a collective agreement.

2.11 Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.

2.12 Processing is carried out by a not-or-profit organisation, provided no disclosure to a third party is made without consent.

2.13 Processing relates to personal data manifestly made public by the data subject.

2.14 Processing is necessary for establishment, exercise or defence of legal claims or where the controller is acting in a judicial capacity.

2.15 Processing is necessary for reasons of substantial public interests on the basis of EU or member state law which is proportionate to the aim pursued and which contains appropriate safeguards.

2.16 Processing is necessary for the purpose of preventative or occupational medicine for assessing the working capacity of employees, medical diagnosis, provision of health or social care/treatment/management.

2.17 Processing is necessary for public health reasons.

2.18 Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

2.19 DPA18 provide certain rights for individuals:

a) Right to be informed;

b) Right of access;

c) Right to rectification;

d) Right to erasure (right to be forgotten);

e) Right to restrict processing;

f) Right to data portability;

g) Right to object

h) Rights in relation to automated decision making and profiling.

2.20 Information supplied about data processing personal data should be concise, transparent, intelligible and easily accessible, as well as written in clear and plain language. Such information should be supplied free of charge.

2.21 Under DPA18 there is no automatic fee payable when a Subject Access Request ("SAR") is made. However, if a SAR is deemed to be manifestly unfounded or excessive a reasonable fee may be charged. FGL will contact the data subject concerned to advise of any such reasonable charges as soon as is practicable once it becomes evident that such charges are appropriate.

2.22 A data request must be honoured within one month, but the controller may be able to extend this period to two months when the request is complex or numerous. However, the individual must be informed, in writing, of any delay within one month, with a clear explanation provided.

2.23 It is possible to refuse to respond to a request if it is excessive or manifestly unfounded, but the refusal must be explained in writing within one month of the request being made.

2.24 If a SAR is made electronically, the information requested may be provided electronically.

2.25 There is no absolute right to be forgotten, and the right of erasure only applies in the following specific circumstances:

a) Data is no longer required;

b) The individual has withdrawn consent;

c) The individual objects to the processing and there is no overriding legitimate interest for continuing the processing;

d) The personal data was unlawfully processed;

e) Personal data has to be erased in order to comply with legal obligations;

f) Personal data is processed in relation to a data subject as a child by social services.

2.26 A request for erasure can be refused on the following grounds:

a) To exercise the right of freedom of expression and information;

b) To comply with legal obligations or for the performance of a public interest task or exercise of official authority;

c) For public health purposes in the public interests;

d) Archiving purposes in the public interests, scientific research, historic research or statistical purposes, or;

e) The exercise of defence of legal claims.

2.27 If an erasure request is honoured, the controller must tell the parties to whom the information has been disclosed unless this is impossible or involves a disproportionate effort.

2.28 An individual can block or suppress processing of their personal data. When processing is restricted, the controller is permitted to store the data, but it should not be processed further.

2.29 The right to object to the blocking or suppressing of personal data applies when the processing is based on legitimate interests or performance of a task in the public interests or exercise of official authority (including profiling), direct marketing (including profiling) (this is an absolute right) and the processing for purposes of scientific/historical/statistical purposes (must be justified on basis there are grounds with regards to the data subject's specific situation).

2.30 The accountability principle in the DPA18 requires controllers and processors to demonstrate compliance.

2.31 There are strict controls over the transfer of personal data outside the EU to third countries and international organisations. Frost Group Limited has a duty to ensure there are adequate safeguards in place to ensure data is only transferred to entities that will comply with DPA18/GDPR and that the personal data will be transferred in a safe way.

2.32 Certain countries outside the EU have been approved by the EU to receive personal data in line with DPA18/GDPR, those countries are Andorra, Argentina, Canada (where PIDEDA applies), Switzerland, Faero Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand. The EU has also approved a Privacy Shield deal whereby from 1 August 2016 US organisations may self-certify to standards required.

3. Data Controllers and Data Processors and the role of Frost Group Limited

.

3.1 Entities which hold personal data are called Data Controllers and entities which process data on behalf of a Data Controller are called Data Processors. It is possible for an entity to be both a data controller and a data processor at the same time.

3.2 Frost Group Limited is a both a data controller and a data processor.

3.3 Insolvency practitioners working for Frost Group Limited are appointed over insolvent entities. It is likely that in most instances that personal data held by the insolvent entity, itself a data controller as well as most likely a data processor, will be retained by it. This will mean that Frost Group Limited may become a data processor for the insolvent entity and will act as agent for the insolvent company as data controller.

3.4 Where insolvency practitioners hold personal data it is most probably for statutory purposes. For instances, to oversee the processing of employee claims by the Redundancy Payments Service, to deal with the unsecured claims of private individuals, to recover book debts due to an insolvent entity.

3.5 Whilst it is extremely unlikely that an insolvency practitioner would be required to take possession of personal data as the data controller when it was not for a statutory purpose(s), where permission to hold such data is required, the insolvency practitioners concerned would need to seek authority from the data subject(s) unless it could be demonstrated that the insolvency practitioner could rely on consent obtained by the insolvent entity prior to the appointment of the insolvency practitioner.

3.6 Where an insolvency practitioner is deemed to be acting as data controller or data processor in respect of personal data held by an insolvent entity, it is deemed appropriate for reliance to be made on consent obtained from data subjects prior to the entity becoming insolvent.

3.7 Where an insolvency practitioner is acting as agent for an insolvent entity which is the data controller or data processor, it is deemed appropriate for reliance to be made on consent obtained from data subjects prior to the entity in question becoming insolvent.

3.8 When an insolvent entity is being traded by insolvency practitioners working for Frost Group Limited all personal data is deemed to be held by the insolvent entity and it is the insolvent entity which will be responsible for ensuring that the correct consent is received from private individuals with whom the business is trading. Frost Group Limited has an internal DPA18 Policy and Procedure for Trading Businesses in Insolvency.

4. How will Subject Access Requests be dealt with by Frost Group Limited?

4.1 Where a SAR is made by a private individual in respect of personal data held by Frost Group Limited itself all such requests will always be processed in line with the DPA18.

4.2 Where a SAR is made by a private individual in respect of personal data held by insolvent entity which continues to trade after the appointment of insolvency practitioners working for Frost Group Limited, we will endeavour to ensure that the insolvent entity concerned complies with the request made in line with the DPA18.

4.3 Where a SAR is made by a private individual in respect of personal data held by an insolvent entity that has ceased to trade it is unlikely that the insolvent entity concerned will be able to honour such a request. This is because it is likely that by the time the SAR is received the Company's records will have either been taken into store or destroyed and the cost of complying with such a request are likely to be prohibitive. It should also be noted that it may be deemed for time costs to be incurred to meet a SAR made by one stakeholder which would be passed onto all stakeholders.

5. How to make a Subject Access Request to Frost Group Limited

5.1 Private individuals looking to make a SAR should write to the Compliance Officer at:

Frost Group Limited
Regus
City South
26 Elmfield Road
Bromley
BR1 1LR

Or email:

enquiries@frostbr.co.uk

A proforma letter is attached as Appendix A

5.2 Where the request is made in respect of an insolvent person or entity the letter should clearly make reference to this in order that it can be quickly referenced to the case in question and processed as quickly as possible.

5.3 DPA18/GDPR do not apply to certain activities including processing covered by Law Enforcement Directive, processing for national security purposes and processing carried out by individuals at home for personal/household activities i.e. Christmas card list/personal address book.

13 March 2020

Frost Group Limited – Subject Access Request Policy and Procedure

Appendix A

Sample request letter

Compliance Officer
Frost Group Limited
Regus
City South
26 Elmfield Road
Bromley
BR1 1LR

Date

Or email: enquiries@frostbr.co.uk

Dear Sir or Madam

Subject access request
Insolvent Entity – in Administration etc

[Your full name and address and any other details to help identify you and the information you want.]

Please supply the information about me I am entitled to under the Data Protection Act 2018 relating to: [give specific details of the information you want, for example

- your personnel file;
- emails between 'A' and 'B' (between Date and Date);
- your medical records (between 2013 & 2017) held by Dr 'C' at 'D' hospital;
- CCTV camera situated at ('E' location) on Date between 11am and 5pm;
- copies of statements (between 2014 & 2016) held in account number xxxxx).

If you need any more information from me, or a fee, please let me know as soon as possible.

It may be helpful for you to know that a request for information under the Data Protection Act 2018 should be responded to within one month.

If you do not normally deal with these requests, please pass this letter to your Compliance Officer. If you need advice on dealing with this request, the Information Commissioner's Office can assist you and can be contacted on 0303 123 1113 or at ico.org.uk

Yours faithfully
[Signature]