YOUR ADDRESS HERE

FORMAL DATA SUBJECT ACCESS REQUEST

DATE:

TO: (by email)

Dear Sir/Madam,

Please accept this as my formal Data Subject Access Request (DSAR) presented to you as per the rights afforded me under the Data Protection Act (DPA) and/or the General Data Protection Regulation (GDPR)

You are hereby requested, as the data controller, to provide all data and information pursuant to me, \_\_\_\_\_\_\_\_\_\_\_\_, the Data Subject, and in respect to any and all business, dealings or communications with me, or in respect to me, from [DATE HERE] up to and including the date of this letter.

As you will no doubt be aware this must include any information about me, whether direct or implied, any opinion of me whether direct or implied and any information that demonstrates or implies any intention of you, the data controller, in respect to me, including how you propose to treat me and any actions you consider or propose in respect to me.

Furthermore, this must include any information that contributes to the formation of an opinion of me, or decision in respect to me, and by all forms of media and communication. This includes all information, notes and communications in respect to the grievance process and investigation.

For the record I refer you the Information Commissioner’s guidance at

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-the-meaning-of-relates-to/#pd1> which states that

“*In many cases data may be personal data simply because its content is ‘obviously about’ an individual. Alternatively, data may be personal data because it is clearly ‘linked to’ an individual as it is about his or her activities and you are processing it for the purpose of determining or influencing the way in which that individual is treated. Data may also be personal data if it is biographically significant or has a particular individual as the focus*.”

This disclosure must include **EVERY** piece of information within your entire files, be they paper, digital or other data format and on any device be it, for example, mobile phone, tablet, laptop, desktop etc. including but not exclusively:

* All communications, notes and statements made internally between you and your employees by any media or format regarding me and any business I conducted with you
* All communications with third parties sent by or received by any of your ‘departments’, your employees and/or your contractors in respect to me, or any matters, issues, complaints etc. involving me, and any business I conducted with you
* All notes taken by any of your employees/contractors in respect to me, and any business I conducted with you, including notes from meetings or following phone calls with me or third parties
* All data and information provided to you by any third party in respect to me, and any business conducted with you.
* A full and complete ‘Statement of Account’ that details every fee, charge or other cost that has been applied to me or my account/payroll with you [DELETE IF NOT APPLICABLE]

To help you with your search for documents please be aware of the following information:

* *INCLUDE ANY INFORMATION HERE THAT MIGHT HELP THEM LOCATE INFORMATION. EMAIL ADDRESSES, HOME ADDRESSES ETC. ORT DELETE THIS SECTION OR DELETE THIS SECTION*

I must remind you that UK data laws and the rights afforded me by them, require you, the Data Controller, to demonstrate the purpose for which this information is being held. This can only be achieved by way of provision of all information in its native format, appropriately redacted ONLY to conceal any information that might be the personal information of third parties.

Given record keeping obligations bestowed upon you by UK Law and regulators, and your awareness that you have a period of 30 days in which you are legally bound to respond to such requests, this request should not be in any way burdensome for you to comply with in its entirety and within the timeframes afforded you.

**I must refer you to the fact that it is a criminal offence under GDPR and the Fraud Act 2006 to fail disclose to me information that you have any legal obligation to disclose to me.**

Furthermore, I refer you to the enclosed Appendix that is ICO Guidance and directives sent to the Data Protection Officer of firm in an Upheld Complaint outcome.

The enclosed guidance, whilst referring to that complaint, makes it quite clear what its general and overriding expectations are of all firms and data controllers and their Data Protection Officers and teams. I am confident that the ICO will not take kindly to their time and mine being wasted by data controllers that wilfully ignore this guidance and directives.

If you have any issue with any aspect of this DSAR, you are afforded 7 days in which to respond and advise precisely as to what they are.

Likewise, if there is any clarity required as to the scope of the DSAR, you are afforded the same 7 days in which to raise the question.

If no issue is raised within said 7 days, it will be accepted that you are processing the DSAR and will comply with the obligations bestowed upon you by the DPA/GDPR within the prescribed timeframe of 30 days.

IMPORTANT: You are reminded that all information requested is entirely confidential and that this DSAR, including the fact that it has been submitted to you, is entirely confidential and must not be discussed or disclosed to ANY third party.

I look forward to receiving your response within the timeframes above.

Regards

**Appendix A –** ICO Guidance and directives sent to the Data Protection Officer of firm in an Upheld Complaint outcome

***“What you need to do now****One of the ICO’s strategic goals is to increase the public’s trust and confidence in how their personal data is used and made available and this relies on data controllers being accountable for their actions in relation to handling data and responding to information rights requests.

Accountability is one of the data protection principles and makes you responsible for complying with the UK General Data Protection Regulation (GDPR).

You must be able to demonstrate your compliance to the complainant and work hard to promote trust and resolve their concerns without the need for the individual to come to us. The attached document provides more detail about this.

As a regulator we look to organisations to effectively manage and resolve the data protection complaints they receive. When an individual comes to us to complain, they are in effect telling the regulator that they believe you are breaking the law. Reports of this kind are something that we will treat seriously and robustly.

We do not expect to receive complaints when there is still further work that you can do to better explain the processing in question to the complainant, or to put things right when they have gone wrong.

We therefore require you to revisit the way you have handled this matter and consider what further action you can now take to resolve this complaint. We expect organisations to deal with the data protection complaints they receive and to proactively work with complainants to provide an appropriate resolution.

If you believe that you have complied with the data protection law, you need to explain this in detail to the complainant. You also need to be confident that you have done all you can to find an appropriate resolution. If your organisation could have done more to resolve the concern then we expect you to take steps now to resolve the issue with the complainant.

I have included a checklist in the attached document to help you with this, you should be able to tick off all the points on this non exhaustive list.

We expect you to contact the complainant within the next* ***28 days*** *with this further detail. If you are unable to meet this timeframe we expect you to contact the complainant to let them know and to advise them when to expect it. You do not need to provide a response to us at this stage.

However, if we receive a further complaint about this processing, we will carefully review and assess the response you have provided to the complainant. If we consider that you are infringing data protection law then we will consider using our formal powers and any sanctions available.

Although individuals do have the right to raise complaints with the ICO, we should not be viewed as a routine second stage in a resolution process. As indicated above, we expect organisations to take their personal data obligations seriously and this should reduce the need for individuals to approach the regulator directly.****Advice and assistance****Our website contains advice and guidance about the processing of personal data and an organisation’s obligations under the Data Protection law. I recommend that you review the information on our website to fully understand your obligations and in particular our accountability framework. We also have specific information about how you should respond to data protection complaints.”*