Mr J Bloggs

Any Street

Any Town

Dear Sir/Madam:

I am writing to you in your capacity as Data Protection Officer (DPO) for your company. I am a customer of yours, and in light of recent events, I am making this request for access to personal data pursuant to Article 15 of the General Data Protection Regulation.

I am concerned that your company's information practices may be putting my personal information at undue risk of exposure or in fact has breached its obligation to safeguard my personal information pursuant to the GDPR.

I am including a copy of documentation necessary to verify my identity. If you require further information, please contact me at my address above.

I would like you to be aware at the outset, that I anticipate a reply to my request within one month as required under Article 12, failing which I will be forwarding my inquiry with a letter of complaint to the Information Commissioner's Office.

Please respond to the following:

1. Please confirm to me if my personal data is being processed. If it is, please provide me with the categories of personal data you have about me in your files and databases.

    a. In particular, please tell me what you know about me in your information systems, whether or not contained in databases, and including e-mail, documents on your networks, or voice or other media that you may store.

    b. Additionally, please advise me in which countries my personal data is stored, or accessible from. In case you make use of cloud services to store or process my data, please include the countries in which the servers are located where my data are or were (in the past 12 months) stored.

    c. Please provide me with a copy of, or access to, my personal data that you have or are processing.

2. Please provide me with a detailed accounting of the specific uses that you have made, are making, or will be making of my personal data.

3. Please provide a list of all third parties with whom you have (or may have) shared my personal data.

    a. If you cannot identify with certainty the specific third parties to whom you have disclosed my personal data, please provide a list of third parties to whom you may have disclosed my personal data.

    b. Please also identify which jurisdictions that you have identified in 1(b) above that these third parties with whom you have or may have shared my personal data, from which these third parties have stored or can access my personal data. Please also provide insight in the legal grounds for transferring my personal data to these jurisdictions. Where you have done so, or are doing so, on the basis of appropriate safeguards, please provide a copy.

    c. Additionally, I would like to know what safeguards have been put in place in relation to these third parties that you have identified in relation to the transfer of my personal data.

4. Please advise how long you store my personal data, and if retention is based upon the category of personal data, please identify how long each category is retained.

5. If you are additionally collecting personal data about me from any source other than me, please provide me with all information about their source, as referred to in Article 14 of the GDPR.

6. If you are making automated decisions about me, including profiling, whether or not because of Article 22 of the GDPR, please provide me with information concerning the basis for the logic in making such automated decisions, and the significance and consequences of such processing.

7. I would like to know whether or not my personal data has been disclosed inadvertently by your company in the past, or as a result of a security or privacy breach.

    a. If so, please advise as to the following details of each and any such breach:

        i. a general description of what occurred;
        ii. the date and time of the breach (or the best possible estimate);
        iii. the date and time the breach was discovered;

iv. the source of the breach (either your own organization, or a third party to whom you have transferred my personal data);
v. details of my personal data that was disclosed;
vi. your company's assessment of the risk of harm to myself, as a result of the breach;
vii. description of the measures taken or that will be taken to prevent further unauthorized access to my personal data;
viii. contact information so that I can obtain more information and assistance in relation to such a breach, and
ix. information and advice on what I can do to protect myself against any harms, including identity theft and fraud.

b. If you are not able to state with any certainty whether such an exposure has taken place, through the use of appropriate technologies, please advise what mitigating steps you have taken, such as

i. Encryption of my personal data;
ii. Data minimization strategies; or,
iii. Anonymization or pseudonymizing;
iv. Any other means

8. I would like to know your information policies and standards that you follow in relation to the safeguarding of my personal data, such as whether you adhere to ISO27001 for information security, and more particularly, your practices in relation to the following:

a. Please inform me whether you have backed up my personal data to tape, disk or other media, and where it is stored and how it is secured, including what steps you have taken to protect my personal data from loss or theft, and whether this includes encryption.

b. Please also advise whether you have in place any technology which allows you with reasonable certainty to know whether or not my personal data has been disclosed, including but not limited to the following:

i. Intrusion detection systems;
ii. ii.Firewall technologies;
iii. iii.Access and identity management technologies;
iv. iv.Database audit and/or security tools; or,
v. Behavioural analysis tools, log analysis tools, or audit tools

9. With regard to employees and contractors, please advise as to the following:

    a. What technologies or business procedures do you have to ensure that individuals within your organization will be monitored to ensure that they do not deliberately or inadvertently disclose personal data outside your company, through e-mail, web-mail or instant messaging, or otherwise.

    b. Have you had any circumstances in which employees or contractors have been dismissed, and/ or been charged under criminal laws for accessing my personal data inappropriately, or if you are unable to determine this, of any customers, in the past twelve months.

    c. Please advise as to what training and awareness measures you have taken in order to ensure that employees and contractors are accessing and processing my personal data in conformity with the General Data Protection Regulation.

Regards,

A.N.Oyed Customer

(Thanks to Constantine Karbaliotis for writing this letter and posting on LinkedIn)