Maslins Ltd re GDPR (General Data Protection Regulations)

As an accountancy firm we hold a lot of personal data relating to clients, both current and historic.

Legal stance

We have reviewed ICO guidance, and our understanding is that we are a data controller. The lawful basis for the data we request/hold from clients is “contract”. Ie we need the data we ask for to do the job you’re paying us to do.

Even after someone leaves as a client, we are still legally required to retain some of that data for things like anti money laundering purposes/HMRC obligations. These take precedence over GDPR. Typically we are required to hold data for 6-7 years after the period data relates to.

Whilst we certainly consider some of the data we hold to be sensitive (in particular bank details, date of birth), from the legal definition within GDPR, none of it is. For GDPR, sensitive data is things like race, political/religious beliefs, health etc. We do not require any of this information, so do not request or hold it.

What we have done

In terms of ensuring as best we can that we comply with GDPR, we have reviewed what data we hold, where it’s held, where it comes from/goes to, and who can access it from where, and how. This has led to us making some immediate changes.

We have deleted some duplicate data from old services we no longer use.

We have reviewed the passwords we use, especially for cloud services where client data is still held, and increased the strength of those passwords where appropriate.

We do believe we require all the data we ask for, and it is all used for the purpose of helping you comply with your accounting and tax obligations. None of it is just for our own interest, or for marketing purposes/sold to a third party.

We have a Mailchimp list which we use for infrequent newsletters (perhaps twice a year around key financial events like tax year end and budget). We believe these are a core part of our offering, so are not specifically requesting clients independently opt in for these. You do of course have the right to unsubscribe if you so wish. We also took this opportunity to remove multiple email addresses of ex clients where we imagine we may no longer have a legal basis to email them without specific opt in, and didn’t want to add to the dozens of pre GDPR emails I’m sure you’ve all received asking you to opt in.

The main places we hold your data

Maslins have an in-office server. A back up of the data is taken daily, encrypted, and saved in a Dropbox account. Some of this data is accessible outside of the physical office location via a VPN.

Many of the services we use are cloud based, hence are accessible from anywhere. We appreciate this makes them vulnerable to inappropriate access. The main such services we use are:

FreeAgent - FreeAgent is of course central to our working with you. Lots of your financial data will be held in your FreeAgent account.

Senta - Senta is our CRM. This includes a database of lots of client standing data. We also use it to help us keep track of accounting tasks for clients. Increasingly we'll be using the client portal side of it, as a way of transferring larger quantities of sensitive data to/from clients.

Our emails go via Gmail's servers. We also use Front to help us share emails internally (eg covering inboxes when staff members are on holiday/courses/ill).

Mailchimp - the data held in here is minimal, but it does include names, company names, and email addresses.

Lots of data relating to you/your business will also be held by Companies House and HMRC.

Who can access what

Maslins staff can access most data on our server from within the office, or remotely via a VPN.

Maslins clients can of course access their own FreeAgent data. Increasingly Maslins clients will also be able to access more of the data we hold for them via the client portal of Senta.

On occasion IT support staff may require access to our server, and/or some cloud based services. We will consider the appropriate way to grant them access on a case by case basis, limit their access to only required areas, and only use providers we trust.

On occasion we take on work experience students from local schools. We take care over what they can access, and take reasonable steps to ensure they only access personal data from within the office, for the period they are working with us.

We will share your data with HMRC and Companies House. Most commonly this will be with your clear permission, following you approving certain items for submission. There may be rare occasions where we are obliged to share data with other law enforcement agencies, eg in cases of suspected fraud/money laundering.

What we will increasingly/continue to do

Whilst GDPR has pushed us to make some key decisions relating to data, we are very much considering this an ongoing process.

We will periodically review where we hold the data, and how secure it is.

We will be gradually reducing the amount of personal data that we email directly to you/request you email directly to us, increasingly moving to using a client portal for exchanging sensitive data. Having said that, we are very aware that for many of you, whilst security is important, convenience is also important. We will therefore be flexible on this, being relaxed about transferring small amounts of not particularly sensitive data via email, but using the portal for larger volumes and/or more sensitive data.

Your rights

You have the right to see a copy of all the personal data we hold for you. We are anticipating that in the fairly near future (though realistically not by 25 May 18) you will be able to see most of the core data we hold for you all the time anyway via your Senta client portal.

Theoretically you have the right to request we delete all personal data we hold for you. However, our understanding is that anti money laundering regulations/obligations to HMRC take precedence over GDPR. In practice this means quite a lot of the data we hold for you, we are legally obliged to retain even if you ask us to delete it. We are therefore within our rights to refuse to comply with requests to delete data.

We will only use your data for the purposes of fulfilling our obligations for you/your business, and legal compliance purposes.

If you have any queries/concerns regarding any of the above, please email info@maslins.co.uk