



DON'T LET YOUR CUSTOMERS' GDPR CONCERNS SLOW YOU DOWN

Five tips to help SaaS providers sign up more customers, more quickly.



WHY YOU SHOULD READ THIS

Workplace digital transformation is being accelerated by the necessity of working remotely due to the COVID-19 pandemic - businesses are looking to software-as-a-service tools to help with this. However, these potential customers for your SaaS workplace solution will (or should) be very mindful of their responsibilities under GDPR to ensure the personal data of their workforce is processed in accordance with the law.

So, if you are a SaaS company which provides tools and services to business customers for their work force, this short guide will highlight what your customer may look for in respect of your GDPR compliance and for which you can prepare in advance. If you are on the front foot with this, it will get a big tick in the box from the prospective customer and get to signature and therefore revenue quicker.

Failure or delay in being able to answer these questions properly and quickly will slow down the process, make you look less professional and perhaps even result in a lost sale.

WHO THIS IS AIMED AT:

Anyone connected with SaaS businesses (particularly workplace solutions) with responsibility for, or an interest in:

- + **marketing**
- + **business development**
- + **sales**
- + **software functionality and development**
- + **data protection compliance**
- + **contract/terms & conditions negotiation**

Please note this short document is written for general guidance only and does not constitute specific legal advice. If you have any questions you should consult a specialist (like us!).



01

SHOW UP FRONT THAT YOU KNOW YOUR GDPR OBLIGATIONS

Customers for your SaaS solution must ensure that their service providers, who are handling their work force personal data on their behalf, offer sufficient guarantees that they can comply with GDPR.

You need to help customers with this due diligence process by being open about your cyber and physical security measures – perhaps in the form of a whitepaper which could deal just with this or indeed widen out more fully to deal with all of the above.

For example, as an absolute minimum your customer will want to know where your platform, and the personal data that it will process, is hosted – if it is outside of the UK or EEA, the customer will have more compliance hurdles to jump over. For more

information on what a white paper might look like, please see [here](#).

You need to know what the customer will want to see in the white paper and how you should address it in a way that will allay any concerns or answer up front any questions they may have.

If you wanted to go the extra mile and show your solution meets benchmark privacy standards, you could illustrate to the customer how the solution meets the “privacy by design/by default” requirements of GDPR. In essence, this means you have to integrate or ‘bake in’ data protection into your processing activities and business practices, from the design stage right through the lifecycle. There are guidelines available for this – for example, [here](#).

02

MAKE SURE YOUR TERMS AND CONDITIONS COMPLY WITH GDPR

Providers and customers are both required by GDPR to ensure that the contract terms and conditions contains certain mandatory clauses.

Make sure you know where and how this is dealt with in your contract. At the same time, make sure you can answer other questions from your customer about whether you have any sub-contractors who process personal data for you. For example, who do you use for hosting - AWS, MS Azure or someone else? Do you subcontract any customer support processes? Being on top of this detail will really help your customer build confidence in you.

You might be tempted to use a template for this or even the customer's own terms and conditions, but if you go down this path, you

will miss the opportunity to minimise your own liabilities and maximise freedom to operate whilst still being GDPR compliant. For example, if you use the customer's own terms, the customer will most likely give itself a veto on your ability to appoint sub-contracts (sub-processors). However, GDPR does allow processors much more discretion to appoint sub-processors even without the customer's consent.

Therefore you want to make sure you give yourself the maximum freedom to operate but still following GDPR otherwise this could hit your bottom line - for example you may want to outsource some support functionality or change to a new cheaper provider. You don't want to be held hostage by the customer.



03

HELP YOUR CUSTOMER WITH ITS OWN COMPLIANCE OBLIGATIONS

Your customer has certain obligations under GDPR to respond to and action requests from individuals about the handling of their personal data - for example, the right for an individual to see a copy of all of his/her personal data held on the platform, or even the right to be entirely erased (“forgotten”) from that platform.

Make sure you know how the functionality of the SaaS platform allows for an individual to action these requests. Is it “self-serve” - for example can a user login to his/her

account and download a full history of his/her activity on that account? Or is it a more manual process (likely requiring your or your customer’s time and resource to manage)?

The extent of an individual’s rights around his/her personal data can be technically tricky and the timeframes within which requests have to be actioned can vary. Implementing these requirements correctly within your platform, systems and procedures is therefore really important.

04

KNOW YOUR STATUS - ARE YOU A CONTROLLER OR PROCESSOR OF YOUR CUSTOMER'S PERSONAL DATA?

You may think it is obvious that just because you are providing a service to a customer that you are automatically the customer's processor. But this may not always be the case where you handle personal data for your own purposes not those of the customer.

For example, if you are aggregating customer personal data to be able to publish a benchmark report across an industry sector - you are doing this for your own purpose not those of the customer.

So you need to assess this and make it clear from the outset whether you are controller or processor (or perhaps both for different kinds of processing).

The terms and conditions where a service provider is a controller rather than a processor are very different. If the customer assumes you are a processor you will be asked to sign up to much more restrictive terms and conditions which will hugely cut down on what you can do with the personal data for your own purposes. So it is vital that you know your status and manage expectations from the outset.

This requires in-depth analysis and knowledge of the guidelines from the regulators to get it right.



05

ASSESS THE RISK

If the processing on your platform could be seen as “risky” in data protection terms (ie it might adversely impact an individual - for example, cause embarrassment or worse, such as affect someone’s credit score) GDPR requires that the customer should carry out a risk assessment - technically termed a “data protection impact assessment”.

What is “risky” personal data is only really identified by way of illustration (for example personal data around health or involving large amounts or personal data). The point of the assessment is to evaluate that risk.

You could help the customer by providing some guidance around how it might complete a DPIA for your service - for example with some of the more tricky questions or fields pre-filled in for the customer to review and then complete.

SUMMARY

The above will all matter to your customers because of the potential damage that can be done to the customer’s reputation if it gets it wrong. A customer cannot avoid liability by saying that its failure to comply with GDPR was all to do with the service provider. Customers have to show that they took all reasonable precautions in appointing a third-party provider. SaaS providers who can help the customer to get to the right answers will thrive.

Helping your customer to help itself will reap dividends when it comes to ensuring a hassle-free contracting process. Data protection can be tricky to get right - applying the broad skeleton of GDPR to your own business and service is not always straight forward and can requires in-depth knowledge of the legislation and any surrounding guidance (which comes out frequently and is often subject to further updates).

HOW CAN WE HELP?

We can help address all of these and allow you to present a whiter-than-white picture to your customers by:

- + ensuring your own data protection and cyber security landscape are GDPR-compliant
- + ensuring your terms and conditions meet GDPR whilst allowing you the maximum leeway permitted
- + providing guidance on your data protection obligations as a controller or processor
- + providing guidance on producing marketing collateral which will help your customer with its own compliance obligations

The next step

The next step is to organise a free GDPR Customer Readiness Assessment so that we can show you where there may be issues to be addressed and how to address them. This process is made up of a questionnaire followed by a consultation.

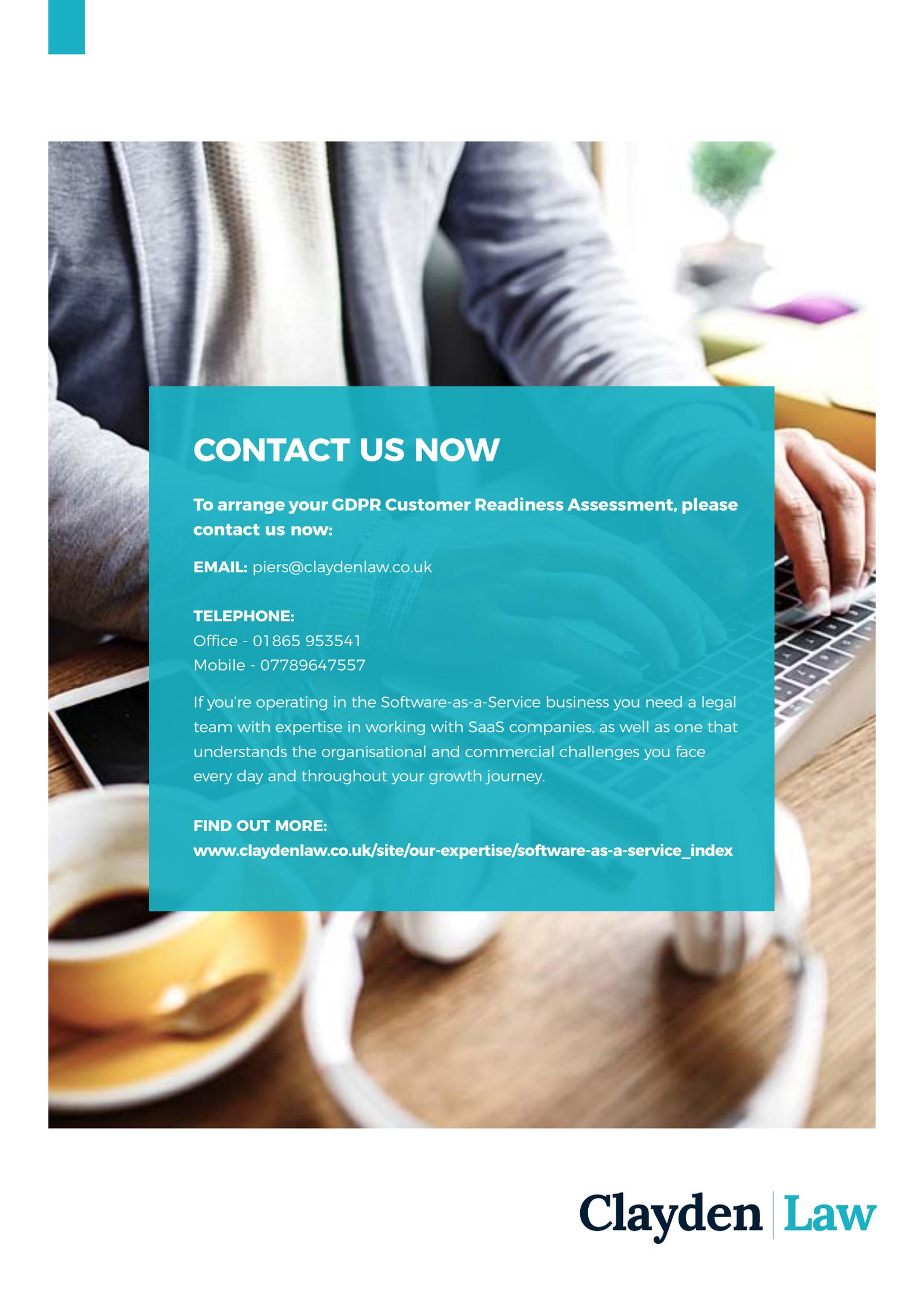
First, you will fill out a questionnaire which will enable us to quickly see where the potential pitfalls might be for you when offering services to your customers.

Then, once you have filled this in, we will organise a 30-minute consultation with one of the lawyers in our data protection team.

Taking this step will result in the following benefits:

- + you will receive expert guidance from experienced data protection lawyers on how any issues identified could be addressed;
- + at the end of the GDPR Customer Readiness Assessment you will have clarity on:
 - + what needs to happen next in order to improve your answers to customers' GDPR concerns; and
 - + what the priorities are so you can start to sign up more customers more quickly.





CONTACT US NOW

To arrange your GDPR Customer Readiness Assessment, please contact us now:

EMAIL: piers@claydenlaw.co.uk

TELEPHONE:

Office - 01865 953541

Mobile - 07789647557

If you're operating in the Software-as-a-Service business you need a legal team with expertise in working with SaaS companies, as well as one that understands the organisational and commercial challenges you face every day and throughout your growth journey.

FIND OUT MORE:

www.claydenlaw.co.uk/site/our-expertise/software-as-a-service_index

MEET THE TEAM



PIERS CLAYDEN

Piers founded ClaydenLaw in 2010. Piers is ranked in the Chambers & Partners Guide, Thames Valley, for his expertise in Information Technology. He is reported as: *Piers Clayden advises both buyers and sellers on a wide range of IT matters, including SaaS and reseller agreements. One client says: "He has the capacity to process a lot of information very quickly and to come forward with commercial propositions that fit neatly within the legal framework."*



HANNAH KIRBY

Hannah has substantial experience of supply of service contracts (in particular cloud-based, SaaS and PaaS services) and research and intellectual property-related agreements, and advised on a diverse range of matters with an emphasis on data protection law, intellectual property and contract-related queries. At ClaydenLaw, Hannah advises on a wide range of technology-related commercial agreements.



ALASDAIR TAYLOR

Alasdair specialises in the law relating to IT. His client work involves drafting, advising upon and negotiating technology-related contracts and other legal documents. His clients include cloud service providers, hosting services businesses, website operators and software developers. They range from newly minted start-ups to established SMEs and international non-profits.



ELIZABETH GIBBS

Elizabeth joined Clayden Law in 2019 and she is particularly interested in advising organisations in the IT sector and those using technology as a fundamental part of their business. Prior to her legal career Elizabeth worked in the education and publishing sectors.



WHAT ONE OF OUR SAAS WORKPLACE SOLUTIONS CLIENTS SAID ABOUT US



((sirenum))

“ClaydenLaw really understands SaaS businesses - not just the legal side but the commercial and organisational challenges, and the steps to take to get things right. Because of their involvement we have been able to improve the way we do things, relax (knowing we’re ticking the legal boxes) and be better equipped for growth and funding rounds. We cannot recommend their specialist experience in this field highly enough.”

WHAT ONE OF OUR SAAS CALL CENTRE TECHNOLOGY CLIENTS SAID ABOUT US



Speik

“We started working with Piers and his team this year and have been hugely impressed with the levels of service and down to earth, commercially focussed advice we have received. We are a rapidly growing company with a large amount of customer contracts to turn around - ClaydenLaw has been able to service our requirements (often under tight timescales) without fuss and always with a sense of humour and a “can do” professional approach. ClaydenLaw has become an essential part of our operation - a partner and trusted adviser relationship, rather than an arms-length lawyer-client one. I would wholeheartedly recommend them as lawyers to any tech company.”

MATTHEW BRYARS, SPEIK’S VICE CHAIRMAN AND CO-FOUNDER



Experts in IT, Data Privacy
and Cyber Security

Clayden | Law