SmartSurvey

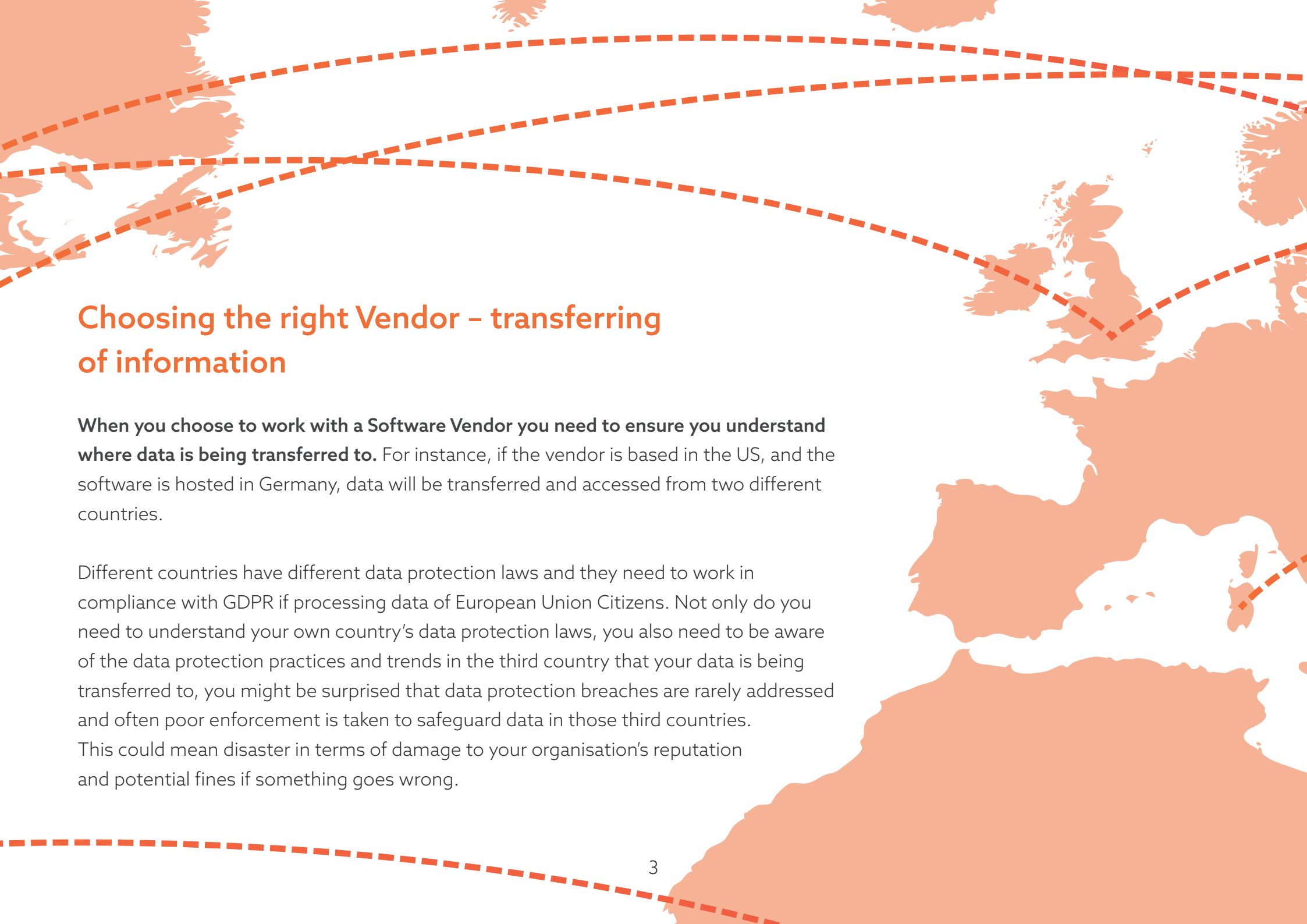
A guide to data security & compliance when choosing a software vendor

www.smartsurvey.co.uk

Data security and compliance

With GDPR now well-established and the potential outcome of Brexit highly uncertain both in terms of timing and detail you should make sure your chosen software partner is fit for the present and the future.

This guide aims to help by explaining the key factors you need to consider when partnering with a software vendor. **By the end of the guide you should have a clearer understanding of what you need to look out for to stay on the right side of data compliance and security when considering to implement a new software solution**.



Choosing the right Vendor – transferring of information

When you choose to work with a Software Vendor you need to ensure you understand where data is being transferred to. For instance, if the vendor is based in the US, and the software is hosted in Germany, data will be transferred and accessed from two different countries.

Different countries have different data protection laws and they need to work in compliance with GDPR if processing data of European Union Citizens. Not only do you need to understand your own country's data protection laws, you also need to be aware of the data protection practices and trends in the third country that your data is being transferred to, you might be surprised that data protection breaches are rarely addressed and often poor enforcement is taken to safeguard data in those third countries. This could mean disaster in terms of damage to your organisation's reputation and potential fines if something goes wrong.

Where does your chosen software vendor store data?

Without understanding local data laws, you could unwittingly be putting sensitive personal information at risk.

For instance, you could be transferring and storing data to a country where the government has the powers to access your data.

Another scenario is a country where low standards of data law enforcement mean criminals could steal your data, with little done to stop or track them down.

Vendors that process personal data outside of the EU, for instance in America, process in accordance with their local regulations. For GDPR compliance, they run a self-certification scheme to demonstrate they comply with GDPR. There are no independent checks, so you will need to have 100% trust in your provider that they are doing things by the book and are compliant.

Check to see where the vendor stores data – ask where their servers are located, and where their backup servers are located. **Backup servers are often continuously processing data, and you may find that these back up servers are in an entirely different country.**

Next, ask where the software team, that will be accessing your data is based? **Are any support and development functions carried out, outside of the UK?** The ICO states that "if an organisation accesses data from a third country, it is technically defined as a transfer." Understanding who has access to your data and from what part of the world is important to understand to ensure compliance.

Top Tip: Ask your vendor to detail the countries where your data will be accessed from, if its outside the UK make sure you are happy with the local laws. Don't forget to ask where their support and development teams are based too as they will also be accessing your data.

What security accreditations does your software vendor have?

You should be looking for an ISO27001 certification. This is an independently assessed certification that demonstrates a software vendor has the correct information security and risk management procedures in place.

An organisation has to apply for the certification, after which an assessment is carried out by an independent body. Once the accreditation is granted, it lasts 3 years, and then the organisation must be re-assessed.

An ISO27001 accredited business is set up to minimise risk, ensure business continuity and ensure all employees follow appropriate behaviour to effectively manage data and reduce the potential for data breaches, cyber-attacks, hack, data leaks or theft.

Another key accreditation to look out for, especially in the UK, is **Cyber Essentials Plus** (or "Cyber Essentials +"). It's a UK government backed scheme and has set the benchmark to minimise cyber-attacks and keep your business safe.

Top Tip: Look out for the Cyber Essentials Plus and ISO27001 badges on your vendors website.

While the lower, "Cyber Essentials" version has become a common accreditation, far fewer software vendors have Cyber Essentials Plus and that is the one that you want.

A key difference is that Cyber Essentials Plus is independently assessed (Like ISO27001) as opposed to the standard Cyber Essentials which is self-certificated. Working with a Software Vendor that is **Cyber Essentials Plus accredited ensures that the vendor has been independently assessed and verified to have the technical and security controls in place to help defend against cyber-attacks.**

Is the software vendor penetration testing?

Penetration testing (also called pen testing) is where an organisation hires a company to carry out "ethical hacking" to identify security vulnerabilities that a genuine attacker could exploit. Ensure that your preferred software provider carries out penetration testing to minimise the chances of attacks and data breaches.

Is your software Vendor Data security and protection tool kit accredited?

The Data Security and Protection Toolkit enables organisations to measure and publish their performance against the National Data Guardian's ten data security standards.

If you are dealing with highly sensitive information such as patient data, you may want to look out for software vendors that have signed up to the Data Security and Protection Toolkit and have obtained a good overall score.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

Think about processing methods in conjunction with your preferred software vendor

If you are engaging with an audience through a software solution, you need to understand the legal basis by which you are processing data. There are 6 of these, the most common you may encounter being having the consent of the subject.

Top Tip: Get your legal department to review data processing agreements, terms and privacy policies before committing to a vendor.

Where explicit consent is being relied on to process data that will be transferred outside of the EU, those transfers outside of the EU need to be mentioned to the data subject as part of that consent. In the post - GDPR world this can have a dramatic impact on engagement levels as many people don't want their personal data leaving the UK.

Is your chosen software vendor flexible with Data Processing Agreements (DPA's)

You'll want to get a copy of your software vendors data processing agreement. You may find there are issues with the way they process data and sub-processors, third parties that process data on their behalf. You want to make sure that, if needs be, they can be flexible on their DPA to be brought in line with your requirements.

Will your software vendor complete an information security request?

Make sure that your software vendor is happy to complete an information security request. Many smaller vendors don't have the processes in place to provide the information required to complete these documents. Subsequently you can quickly identify if there is potential that your data could be at risk. **Many larger vendors will not usually agree to fill out information security documentation and instead direct you to a generic page on their website, thereby giving you little assurance.**

Does your chosen software vendor offer single sign on?

Check to see whether your vendor can offer single sign on (SSO). Single sign on can make management of data access far simpler as its linked though a windows feature called Active Directory via the SAML protocol. The process of managing leavers and new joiners is streamlined and centralised through IT. This in turn ensures unauthorised access to data is minimised as login details will be revoked as soon as IT remove their Active Directory entry.

Can your software vendor provide access restriction via IP?

Access restriction via IP is a particularly useful feature. It helps to reduce the surface area for potential attacks by restricting logins to a set or group of IP addresses. Once in place users can only access their account from a specific IP. Trying to access from a non- specified IP will result in them being unable to login.

Does your Software Vendor include Two-Factor Authentication?

Post GDPR all companies are becoming increasingly data savvy. The threats of data theft from cyber-attacks, phishing attempts and account hacking are real, and the penalties for breaches are significant. That's why many companies are partnering with vendors that can include two-factor authentication (2FA) in their login process.

2FA works by the user being asked to input a one-time passcode which is sent to their mobile device.
This process is strong at stopping weaknesses in systems that hackers and fraudsters exploit such as stealing login credentials.

Why is 2FA so effective at improving system security?

It's effective because the login credentials are no longer enough to access the system. The attacker also needs access to the linked device. Without this, they cannot receive the unique one time pass code sent to it. This code will expire after a set time, increasing security.

This all makes accounts harder to spoof – attackers can register false accounts or try to gain access with stolen login details but **it's extremely hard for them to get the details of the unique device that would receive the one time pass code to login.**

Make a #Smartmove and choose SmartSurvey

SmartSurvey is UK hosted, and our entire team is UK based. You can be confident that we comply from a storage and transfer perspective, and all data is only accessed by UK staff.

We have multiple security accreditations:

- ✓ ISO27001
- ✓ Cyber Essentials +
- ✓ Data protection and security toolkit

Good to know...

- ✓ We are happy to provide custom Data Processing Agreements (DPA).
- ✓ We regularly complete information security requests.
- ✓ Government Approved G-Cloud Supplier
- ✓ Regular Penetration Testing

Additional security functionality we provide:

- ✓ Single Sign On
- ✓ Restricted IP Access
- ✓ Two factor Authentication

In short, now more than ever, you need to care about how data is processed, stored and transferred and the level to which it's protected.

You need to ensure you have confidence that when you partner with a software vendor, they are compliant. Not doing so could be the difference between processing your data lawfully or receiving a fine for a breach which could be up to 4% of annual global turnover or €20 million – whichever is greater.

Make a #smartmove and choose SmartSurvey.

SmartSurvey Ltd
Basepoint Business Centre
Oakfield Close
Tewkesbury
Glos. GL20 8SD
United Kingdom

0800 0937 822 sales@smartsurvey.co.uk www.smartsurvey.co.uk