Vol. 3

Start-up guide | Data Privacy

7 key points to protect personal data and be compliant with the General Data Protection Regulation

KROMANN
REUMERT

Read our other start-up guides

If you're also interested in the rest of our start-up guide, please just ask us for a copy of Vol. 1 about getting ready for investments and Vol. 2 about the rights of your start-up and how to avoid violating the rights of others.

Hi there!

We know that you'd probably rather spend your time working on your new idea, so we won't take up much of your time. But we really want to see you succeed with your start-up, and it's our experience that data protection requirements affect all businesses. Compliance can be a challenge for start-ups, which is why we've made this third chapter of our start-up guide.

Protecting personal data is the new black. People are talking about it, customers are demanding it, and it's all over the media. If you get it right, your brand and reputation will prosper. If you get it wrong - well, you do the math. But also, non-compliance with the General Data Protection Regulation, also known as the GDPR, and other regulation on the processing of personal data could potentially cause considerable sanctions for you. And it could cost you in terms of lost customers or lower valuations by investors.

The most important thing is to know what processing of personal data takes place in your start-up and why: Purpose is king under the data protection rules. Some of the potential issues can be resolved easily and at no cost, while others may be somewhat more complex and expensive. In this regard, we stress that it is always easier and less expensive to have these matters sorted early on than having to fix things once problems begin to arise.

To help you get a quick overview of the most important aspects to consider when you handle personal data, we've drawn up 7 key points that we hope you'll consider and keep in mind as you accelerate your start-up. And just remember: Protecting personal data is about protecting the fundamental rights of people, including yourself.

We love working with start-ups, and we'd be happy to meet you for an informal discussion (free of charge, no strings attached) on your thoughts, concerns, hopes, and wishes as a start-up, and to advise you on how to best prepare from a legal point of view. So please, feel free to contact any of us – you'll find our contact information in the back of this leaflet.

#1

Map your data. Where, why, and how?

In short, "personal data" is any form of information which directly or indirectly relates to an identifiable person. It could be anything from a name, to health information, or even your customers' shoe sizes. Processing means any interaction with personal data, from collecting them, to deleting them, and even just having digital access to them. Any processing of personal data will be subject to restrictions and requirements.

To get data protection right, you need to first map out the data flows of your start-up. If you don't know where, why, and how you are processing personal data, and what types of data they are, you cannot protect the data properly. Your start-up will very likely be required to have records of your processing activities, but even if that is not the case, it's still a good idea. Mapping your data gives you an overview, provides a basis for protection, and can be used as documentation. You should know that in certain industries - health and telecom, for example - personal data is more extensively regulated.

#2

Build in data protection right from the start!

It is often cheaper and more expedient to incorporate data protection in your business concept, software, and platform from the start. Therefore, when you start your business, think about what role personal data play and if there's any way you can minimize the amount of personal data processing. You should do this every time you develop a new product. It is much simpler than striving for compliance later on.

#3

You don't always need consent

It's a common misunderstanding that any processing of personal data requires consent. This isn't always the case. It depends on the type of personal data processed and the purpose of the processing. When your start-up processes ordinary personal data about a data subject such as name, telephone number, and email, you will normally not need to obtain consent. In most cases, such personal data may be processed because it is necessary to perform a contract, to meet a legal requirement, or your legitimate interests in processing the personal data override the interests of the data subject. However, be cautious - it can be difficult to assess the appropriate legal basis for processing.

If you do need consent for a processing activity, you can obtain it digitally through a click box on your website or app. The text by the click box must be clearly worded so that the data subject knows what is being agreed to. You can choose to put the text in a privacy policy and provide a link by the click box. A specific purpose must be stated (see advice #1), it must say that the consent can always be withdrawn, and it must be clearly distinguishable from other matters. Consent may always be withdrawn, and it must be just as easy to withdraw as it was to give. Oh, and you must always be able to demonstrate that the data subject has given consent.

Even if consent is not required, you must always inform about the processing activities. Please see advice #4.

#4

Your duty to inform - and other rights of the data subject

The data subject must always be informed before any processing of personal data. And, as with requests for consent, the wording must be clear. It's practical to give this information when collecting the data from the data subject, e.g. from your web shop.

The information can be given easily through a privacy policy on your website, but never forget that it must be easy to understand.

If processing goes beyond the originally stated purpose, the data subject must be notified again. Data subjects also have other rights, like the right to access their data or to have their data rectified, deleted, transferred to a third party (if technically possible), etc.

#5

Do your suppliers have access to your personal data?

An entity which processes personal data is either a controller, a processor, or both in relation to each processing. When it is your start-up determining why and how data is processed, your start-up is the controller in relation to such data. Controllers have all the duties listed in the first 4 key points of this leaflet, and they must be able to demonstrate compliance.

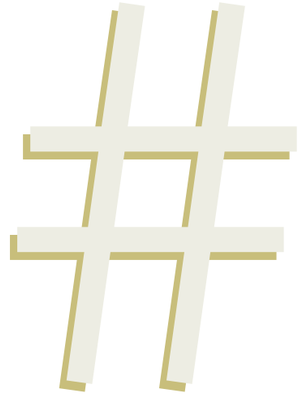
You may allow your suppliers of software and hosting access to these data. If you do this, those suppliers will become processors in regard to the personal data that you control and must, as such, be instructed on how to process the data. The instructions, by legal requirement, must be given in a so-called data processing agreement. A template can be found at the Danish Data Protection Agency (Datatilsynet) website - both in Danish and in English. A practical solution would be to incorporate this in the agreement you make with your suppliers.

You can only allow suppliers access if they sign the data processing agreement and if they can demonstrate that they will also comply with data protection rules and regulations. You should be particularly alert in regard to free software providers, whose business models often depend on data.

#6

Are you also a processor?

Similar to the situation in advice #5, your start-up may also process personal data on behalf of other businesses - your customers, for example, if you trade in, say, software or hosting. As a processor, you must be able to demonstrate compliance with data protection rules, and you must enter into data processing agreements with the controller. Remember, that you are acting on the instructions of the controller.



#7

Privacy by design and default - information security

Information security and data protection go hand in hand. Whether you're the controller or processor, you must use adequate means to protect personal data.

You must also do privacy by design and default. This means that when you develop new products or technologies that involve any kind of processing of personal data, they must always be designed in a way that affords an appropriate level of data protection, and the security settings must be set to the highest possible data protection by default. This requirement is relevant to anyone developing products that process personal data - which may include products such as wearables, apps, servers, sensors, hardware and software robots, AI, platforms, and much else.

Contact

Do you have any questions or need help?
Feel free to write or call us for an informal talk or meeting – free of charge and with no strings attached.

Torben Waage
Partner
Dir. +45 40 61 08 86
Mob. +45 38 77 45 60
tw@kromannreumert.com

Kristian Storgaard
Partner
Dir. +45 38 77 44 70
Mob. +45 20 19 74 10
kst@kromannreumert.com

Sara Goul Ærthøj
Director, attorney
Dir. +45 38 77 12 66
Mob. +45 30 83 42 37
saae@kromannreumert.com

Heela Lakanval
Senior Attorney
Dir. +45 38 77 46 61
Mob. +45 61 55 21 94
hlv@kromannreumert.com

KROMANN REUMERT

At Kromann Reumert, we set the standard. Together. We provide value-adding solutions and advisory services with dedication and focus. We are driven by our four core values: quality, commercial understanding, spirited teamwork, and credibility. We are Denmark's leading law firm with offices in Copenhagen, Aarhus and London.

COPENHAGEN
Sundkrogsgade 5
2100 Copenhagen Ø, DK

AARHUS
Rådhuspladsen 3
8000 Aarhus C, DK

LONDON
65 st. Paul's Churchyard
London EC4M 8AB, GB

LAW FIRM
kromannreumert.com
Tel +45 70 12 12 11