www.jusletter-it.eu

Daniel Ronzani

Are You GDPR-compliant? GDPR-what!?

Category: News
Region: Switzerland
Field of law: Data Protection

Citation: Daniel Ronzani, Are You GDPR-compliant? GDPR-what!?, in: Jusletter IT 24-Mai-2018

ISSN 1664-848X, https://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

[Rz 1] In the past few months we received several enquiries from small and medium enterprises (SME) with statements like: «*We received a processor contract from our customer for sign off. Can we sign it? And, by the way, we also want one of these to be GDPR-compliant*».

[Rz 2] The burden of implementing the General Data Protection Regulation (GDPR) is high for SME[1]. Formally, GDPR contains 173 Recitals and 99 articles on 88 pages. Materially, processing of personal data includes principles such as, for instance, transparency, purpose limitation, accuracy, data minimisation, integrity and confidentiality, or accountability (art. 5 GDPR). So «*one of these*» alone will not make you GDPR-compliant. Being GDPR-compliant does not mean merely posting a GDPR-compliant privacy policy on your website; although, visibility of GDPR-compliance is a first important step.

[Rz 3] I summarize four *selected* points you might consider towards GDPR-compliance:

1) **Documentation**: You should evaluate and document the personal data you process. Before you can prepare any privacy policy and processor contract, as the case may be, you need to know what personal data you process. You most probably have personal data in your HR department (employees/freelancers), procurement department (suppliers), sales department (customers), or from third parties (web users), etc. The granularity of detail is high. For each data list you should know what personal data you process for what reason and with what justification. For instance, your website customer, who purchases merchandise, will necessarily provide his or her name, address, e-mail and credit card details. He or she might also provide additional personal data voluntarily, e.g. birth date.
2) **Technology**: You should evaluate (and reduce according to the principle of data minimisation) the technology you implement. If, for instance, you provide services over the Internet, your website might integrate technology such as cookies, pixel-tags and social media plug-ins. With these technologies you can track and assess the online movements and preferences of web users. Ask yourself whether you actually need this information to provide your services. Chances are that you do not require this information and that statistics you might want to draw from your web users can be computed with anonymized and aggregated data.
3) **Processing**: You should evaluate from where you receive personal data and for whom you process them. It is important to know whether you receive personal data you process directly from the data subject or from a third party. You also need to know whether you process personal data for your own purpose or on behalf of a third party. A party providing (third party) personal data to you will require you to give guarantees that you, for instance, only process them as instructed. Likewise, if you engage a subcontractor for processing personal data you received, you will want to receive such guarantees. Once you have assessed this information, you will be able to prepare a processor contract.[2]
4) **Justification/Retention**: You should evaluate the justification for processing personal data. As a general principle, data processing is not permissible (art. 6 GDPR). You need a justification for processing personal data. A justification can be, among others, performance of contract, consent, compliance with the law, public interest, or archiving. You need to know the basis upon which you are processing personal data. For instance, you must retain

1 Niklaus Nuspliger/René Höltschi, Was Sie über die Zeitenwende im EU-Datenschutz wissen müssen, NZZ vom 17. Mai 2018 (tinyurl.com/yc3wwtym).

2 For details, see: Simon Schlauri, Auftragsdatenverarbeitung nach DSGVO, in: Jusletter IT 24. Mai 2018.

relevant personal data from your web customer for ten years as required by commercial accounting and financial reporting regulations (art. 958f Code of Obligations [CO]).

[Rz 4] I recommend summarizing the information in points 1–4 (and possibly more) in a document, for instance an Excel sheet. This will not only help you prepare a privacy policy that fits your individual processing of personal data and also enable you to assess what other contractual rights and obligations you need to give and receive for data processing but also bring you a step closer to GDPR-compliance.

Daniel Ronzani