GDPR CHECKLIST

streampoint SOLUTIONS

Event Registration Made Simple!

Expectation

GDPR stands for the General Data Protection Regulation. In some respects it could be thought of as the Global Data Protection Regulation, because it also affects businesses outside Europe.

Expect that your organization is subject to GDPR compliance. While you may not physically have a presence within the EU, your organization most likely deals with, in some manner, the personal data of a number of EU nationals (which we'll refer to as 'data subjects'). The GDPR defines people or organizations who collect and manage personal data as 'data controllers.' Further information on the definition of a data controller can be found here: (http://ec.europa.eu/justice/data-protection/data-collection/index_en.htm)

☐

Don't assume that you're automatically compliant or worse yet, sit idly by hoping it will just go away. GDPR is here to stay! Legislation is already in place but goes into force on May 25, 2018 and there are large penalties in effect for non-compliance. Penalties for non-compliance are set in two tiers:

Tier 1 - Fines of up to €10 million or 2% of total worldwide annual turnover (remember, that's revenue - not profit!) can be levied for more administrative infringements.

☐

Tier 2 - Fines of up to €20 million or 4% of total worldwide annual turnover for more serious infringements. In either case - both are high so be warned and be prepared!

Education

Keep your head out of the sand! Ignorance is not an option or an excuse for not complying.

Develop training for employees, senior management and key decision makers within your organization on the topics GDPR governs such as data protection and the rights and freedoms of data subjects.

☐

Stress the severity of penalties and the potential damage and disruption to your organization should it not comply with GDPR. Calculate the potential fines for your organization at both tiers and show them should you encounter resistance for implementing GDPR compliance measures, as it's highly likely the fines will be more costly.

☐

Evaluation

Get a bird's eye view of your organization's data.

Audit your organization's data systems and assets from end-to-end to determine where personal and sensitive data is located. A data stream map is a good way of documenting all of the personal data processed within your organization and where it flows and is stored. Include mobile devices, data systems and assets that are outside of your organization's direct control (such as Dropbox, etc) and third party vendors you have agreements with who may be handling / processing some of your organization's data. Basically, know where all your data goes! ☐

Ensure your audit also encapsulates staff within your organization in terms of who has access to personal and sensitive data and whether permissions are appropriate or need to be revised. ☐

Evaluate software and/or processes geared towards discovery of data breaches and for rapid response and intervention into breach attemptions by malware, unauthorized access, etc. It won't look good for your organization if you don't know you've been breached, aren't aware of when or how it happened or worse still if it's made public by another party. ☐

Establishment

Enact data handling processes so there's a place for everything and everything has its place.

Implement procedures and best practices for the handling of personal and sensitive data. Be sure to align them with GDPR requirements. These also need to be documented. Not having accurate documentation of your organization's data processing and its handling of personal and sensitive data can be construed as a Tier 1 offence under the GDPR legislation and could be costly. ☐

Use this opportunity to modify or do away with those processes that are redundant or not compliant with GDPR - after all, spring cleaning is a good thing! ☐

Determine whether your organization is required to appoint a Data Protection Officer (DPO) based on Article 37 of the GDPR legislation. Even if your organization does not require a DPO to be appointed as a specific role, there does need to be a contact accessible for EU data subjects to exercise their right to be forgotten, enquire about or amend their consent to the use of their personal data. ☐

Encryption

Great - you've gotten your data ducks in a row! Now you need to keep them protected.

One of the strongest protection measures highlighted in the GDPR is data encryption. If your organization is not doing this already, look into implementing encryption / pseudonymization for your data. ☐

Investigate device management tools that can remotely wipe and/or kill mobile/external devices that are lost, stolen, misplaced or otherwise similarly compromised. Loss of devices is one of the major causes of data breaches as they are relatively easily accessed and unlocked. ☐

If you haven't done so already, invest in and install anti-malware to protect your data by blocking malicious software. ☐

Exposure

The commonly held view of data breaches occurring is not a case of 'if' but rather 'when'. It's too late to scramble to put processes in place once a breach happens so be prepared ahead of time!

Determine, based upon your data audit and implementation of data protection tools, what would constitute a breach and develop your organization's response plan. The GDPR defines a breach as *"accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."* ☐

If a data breach occurs the local GDPR Data Protection Authority and all affected data subjects must be notified within 72 hours as its the extent, the potential fallout and also the remedial action being taken. *(A Data Protection Authority is setup in each EU member state, and at the time of publication of this guide still pending outside the EU. Contact details for each Data Protection Authority can be found here: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm)* ☐

Also if a breach occurs, it may have damaging repercussions for your organization's reputation. Consider engaging the services of a PR firm to advise or have a standing agreement with one in place should you need to go into damage control. ☐

Elevation

GDPR takes your interaction with users to a whole new level.

Recognize that GDPR now carries an elevated level of consent required from data subjects. User consent forms should be in clear and plain language and not be implicit, employ pre-checked boxes or assumptive means (i.e. opting out rather than opting in) of obtaining consent. The GDPR defines consent as *"any freely given, specific, informed and unambiguous indication of the data subjects' wishes…by a statement or a clear affirmative action [that] signifies agreement to the processing of personal data relating to him or her."*

☐

Respond to requests from data subjects in a timely manner as they have right of access under GDPR to determine the purpose behind their personal data processing, i.e, who will receive it, how long the data will be stored and more. Other rights users have is the right to correct inaccuracies in their personal data. Articles 13-15 provide rights to the data subject to be able to receive *"meaningful information about the logic involved".* Initial requests for information from the data subject should be provided free of charge, however the legislation does allow for a levying of *"a reasonable fee based on administrative costs"* for further copies requested.

☐

Endgame

What to do once your organization is compliant.

Keep assessing the processes you've put in place - compliance is an ongoing process. Whilst having IT/security tools in place is a necessary part of GDPR compliance, they themselves are not a silver bullet and will not automatically make you compliant.

☐

Advocate for and help institute GDPR compliance across the board. Reach out to your technology partners and find out whether they're compliant or not.

☐

Disclaimer: *Please note that the information contained within this document is intended as a guide only and should not be substituted for legal advice. Streampoint Solutions Inc. makes no warranties, expressed, implied or statutory as to the information in this document. This content is provided 'as-is' and as such the information and views expressed in this document are subject to change and may do so without notice.*

There's a **full service registration solution** behind every click.

Online Registration	Housing Management
Onsite Registration	Integrated Beacons
Lead Retrieval	Integrated Mobile
Booth Management	Integrated CRM / AMSa

streampoint SOLUTIONS

1.866.464.3339
streampoint.com
sales@streampoint.com

Streampoint is an event registration company founded on the principles of delivering proven, reliable and innovative solutions for your event. Think of us as the problem solver for your event's technological speed bumps.