Data Protection Guidelines

Objectives:

- ☑ To share "DOs" and "DON'Ts" concerning the processing of personal data shared by Web Summit in the context of Conferences; and

- ☑ To share guidelines and data protection rules, based on applicable legislation, that can be useful for our partners, startups, VCs, among other external stakeholders ('stakeholders') in ensuring and enhancing data protection compliance.

List of Contents

I. Applicable legislation

Web Summit is a global organisation headquartered in the European Union and subject to applicable European regulation. Its main processing activities are regularly conducted in the European Economic Area (EEA) and, therefore, subject to the **General Data Protection Regulation (GDPR)** as a general rule.

As we orchestrate Conferences in different parts of the world, other data protection legislation may also apply in addition to the GDPR. In that sense:

- The **Brazilian General Data Protection Law (LGPD; Law 13.709/2018)** is applicable to processing activities in the context of Web Summit Rio;

- The **Personal Information Protection and Electronic Documents Act (PIPEDA)** is applicable to processing activities in the context of Collision; and
- The **Personal Data Privacy Protection (PDPP; Law 13/2016)** is applicable to processing activities in the context of Web Summit Qatar.

a. Why is this relevant to our stakeholders?

Web Summit's processing activities include, although it's not limited to, the personal data sharing with external stakeholders for multiple purposes (*as described in our Privacy Policy!*).

Therefore, the applicable legislation will have an impact on how they will be able to handle the shared personal identifiable information (PII), as well as on the contract to be signed between the interested parties, as their data protection terms may need to be localised and adjusted in view of the applicable legislation (e.g., MSA, Single Event Agreement, Order Form, etc.).

II. Data protection roles

In the Data Protection realm, the key players that generally process personal data are:

- **Controller / Independent Controller**: Means the natural or legal person, public authority, agency or other body which (independently) determines the purposes and means of the processing of personal data.
    - **Joint controllers**: Means the natural or legal person, public authorities, agencies or other bodies which jointly determines the purposes and means of the processing of Personal Data.
- **Processor**: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- **Sub-processor**: means a natural or legal person, public authority, agency or other body which acts under the instructions of the processor and processes personal data on behalf of the processor.

a. What are the roles & responsibilities of Web Summit & its stakeholders?

As a general rule, Web Summit and its stakeholders are independent controllers because each party processes personal data for their own purposes.

In exceptional cases, a joint controllership may be established when/if common projects and initiatives are organised by the interested parties (e.g., side-events; etc.). However, this is normally not the case.

III. Handling the personal data shared by Web Summit

a. For what purposes will Web Summit share personal data with stakeholders?

Web Summit may share personal data with stakeholders on limited occasions when this is required for the fulfilment of certain purposes, such as organising an initiative in the context of a joint controllership (**exceptionally*), or providing attendees with the promised services and/or products, as specified in our Terms and Conditions (T&Cs) and Privacy Policy.

Web Summit may also give access and/or share personal information withstakeholders for marketing purposes. However, this is only done when **express consent** is provided by the data subject (i.e., *attendee*) - *as further specified below.*

b. When will Web Summit share personal data with stakeholders for marketing purposes? What process is in place?

Web Summit does not share personal data with stakeholders for marketing purposes, unless the data subject has provided explicit consent.

The consent can be provided in two forms:

1. When the data subject accepts invitations from connection requests coming from the stakeholders' profiles in the Web Summit App.

   → When an attendee clicks on "accept connection request", a central pop-up banner appears, containing a marketing consent clause which can be then accepted or rejected.

   This clause informs the data subject that their personal data will be shared with the corresponding stakeholder for marketing purposes.

   It also clarifies that the personal data will be handled independently, in accordance with the stakeholder's policies & practices, and that they may unsubscribe at any time by contacting the respective stakeholder.

2. When the data subject allows a company to scan the QR code visible on their lanyard and/or when the data subject scans the QR code from a company (i.e., partner, startup, VC, etc.).

   → When the data subject provides this authorisation and/or proactively connects with a stakeholder, the same central pop-up banner appears on their App page.

   Once again, the information specified above appears and the data subject has the opportunity to either accept or reject the connection.

c. How is the collected/authorised personal data shared by Web Summit?

Every time an attendee accepts to connect with a stakeholder, their contact details (*including their email*) are added to a list that is accessible by the third-party via the Web Summit App.

This list can be exported and downloaded by the stakeholder and the data can be added to their database subsequently.

d. What are the differences between "attendee to attendee" connections vs. "company to attendee" connections? Can an attendee collect marketing consent on behalf of their company from their personal app profile?

"Attendee to attendee" connections are connections at a personal level. They are aimed at allowing attendees to individually interact with each other, for their own personal networking purposes.

The personal data shared between attendees in that context must be used by the affected attendees **only** and shall **not** be shared with organisations (partners, startups, VCs, etc.) for any type of further processing, even if the attendees are employees and/or representatives of an organisation/company.

In other words, any personal data gathered and/or shared in the context of "attendee to attendee" connections cannot be used for an organisation's marketing purposes.

On the other hand, "company to attendee" connections are aimed at allowing organisations to collect marketing consent from attendees. "Company to attendee" connections can only occur when the connection is done between an attendee profile and a company profile (i.e., *the institutional profile of a partner, a startup, a VC, etc.; and* ***not*** *the personal profile of its representatives and/or employees!*[1]).

When an attendee connects with a company profile, the process described in subsection "b" (above) is triggered.

[1] Profiles of employees and/or representatives of a company are deemed to be personal profiles and **not** company profiles!

The personal data collected in the context of "company to attendee" connections can be used for the marketing purposes of the **specific** stakeholder that connected with the attendee. It cannot be shared with other companies and/or affiliates (*even if from the same corporate group!)* for their marketing purposes.

e. What is the lead scanning feature?

The lead scanning feature gives stakeholders the opportunity to manage their tickets and give their ticket holders the possibility to collect marketing consent (*scan leads!*) on their behalf.

In other words, if a stakeholder activates this function for a certain ticket holder, the ticket holder will be able to collect marketing consent on behalf of the stakeholder **via their company profile** on the app, by scanning other attendees' lanyards (i.e., *their QR codes*).

In such a scenario, the marketing consent would be collected via the company profile and not the personal profile![2]

Every lead collected in this context is also added to a list containing attendees' contact details (*including their email*), that is accessible by the respective stakeholder via the Web Summit App.

The ticket holder who has the lead scanning feature activated and, therefore, collects marketing consent on behalf of the third-party ***can also have access to the collected data***!

[2] The attendee receiving the connection request would only view the company's profile! I.e.: "["COMPANY"] wants to connect with you!"

f. How to activate the lead scanning feature? What are the usage rules?

The lead scanning feature is deactivated by default. It can be activated by the stakeholder on the ticket dashboard.

Each stakeholder is *responsible* for deciding which ticket holders will have access to this feature, in view of our T&Cs.

In other words, some ticket holders may have it activated and others shall not. This is managed by the stakeholder, in line with applicable rules.

Ticket holders with an active lead scanning function will have access to the personal data collected on behalf of the stakeholder, as specified in the section above.

Therefore, stakeholder **can only activate this function if the ticket holder is their direct employee and/or is a documented representative of the organisation** (*with established contractual obligations, particularly concerning confidentiality and data protection compliance*).

Non-compliance with this rule is a violation of our T&Cs and Privacy Policy, as well as of applicable data protection legislation. Please learn more about potential sanctions in sections "h" and "i" below.

g. Are stakeholders allowed to bypass the 'express consent rule' to collect personal data for marketing purposes? Can they scan the QR codes without asking for permission first? Can they perform "web/app scraping" and/or independently harvest contacts on the Web Summit App?

No. Collecting the referred personal data for marketing purposes with no applicable legal basis (**explicit consent*) is not only a violation of our T&Cs and Privacy Policy, but it's also an unlawful processing of personal data under the GDPR and the other applicable data protection legislation listed under section I (above).

Please learn more about potential sanctions in sections "h" and "i" below.

h. What are the penalties for non-compliance with Web Summit's policies?

Non-compliance with Web Summit's policies is a material breach punishable with contractual and/or package termination.

In such circumstances, Web Summit may proceed to the referred termination immediately at any time by written notice to the stakeholder, and it shall not be required to refund any fees received from the third-party.

Web Summit shall be entitled to submit an invoice in respect of the balance (or the whole as the case may be) of fees which will become immediately due and payable and it will not be liable to the stakeholder for any loss or damage of any kind resulting from such a termination.

Web Summit may also refuse to celebrate new agreements and/or sell packages concerning future Conferences to stakeholders found to have breached and abused its policies, and applicable data protection legislation.

Finally, the respective stakeholder will hold Web Summit harmless from any losses and damages due to any breach, whether by action or omission, regardless of fault, in the processing of the referred personal data.

Learn more on our T&Cs.

i. What are the penalties for non-compliance with applicable data protection legislation?

Non-compliance with applicable data protection legislation can lead to loss of customer trust, reputational damages, civil liability (*e.g., claims raised by data subjects*),

external scrutiny by competent authorities and severe administrative fines[3], among others.

Considering our stakeholders are independent controllers, they are independently responsible and liable for any breaches and/or violations they may cause, by action or omission, and regardless of fault, in the processing of the referred personal data.

Web Summit's policies are aimed at fostering compliance and championing privacy!

Therefore, we strongly advise stakeholders to comply with them at all times and, when in doubt, consult with your legal and data protection teams before any processing of personal data is carried out.

Web Summit also advises stakeholders to avoid processing personal data unlawfully at all times, particularly in what concerns direct marketing.

We make our best efforts to monitor compliance during our Conferences and to filter stakeholders that are committed to the highest standards of legal conformity - *just as we are*!

j. As independent controllers, what are the responsibilities of the referred stakeholders & Web Summit?

Each independent controller is individually responsible for ensuring compliance with applicable data protection legislation when processing personal data for their own purposes.

In this particular context, for example, this includes but is not limited to:

[3] Under the GDPR, fines can go up to €20 million or 4% of the organisation's annual worldwide turnover (*whichever is higher*).

- ☑ Keeping track of collected consents & unsubscriptions, and sharing the respective marketing communications accordingly (**consent management*);
- ☑ Providing data subjects with a Privacy Notice and clear information on how they can exercise their data protection rights;
- ☑ Ensuring data subjects will have their rights & requests fulfilled whenever possible and/or required by law;
- ☑ Informing data subjects about the fulfilment or denial of their requests, as well as of the reasons for denial (**if that is the case*);
- ☑ ***Among others*!**

Independent controllers have the same obligations that controllers would normally have in respect to the processing of personal data. Developing a robust **data privacy framework & culture** in the organisation is strongly recommended to achieve and maintain compliance.

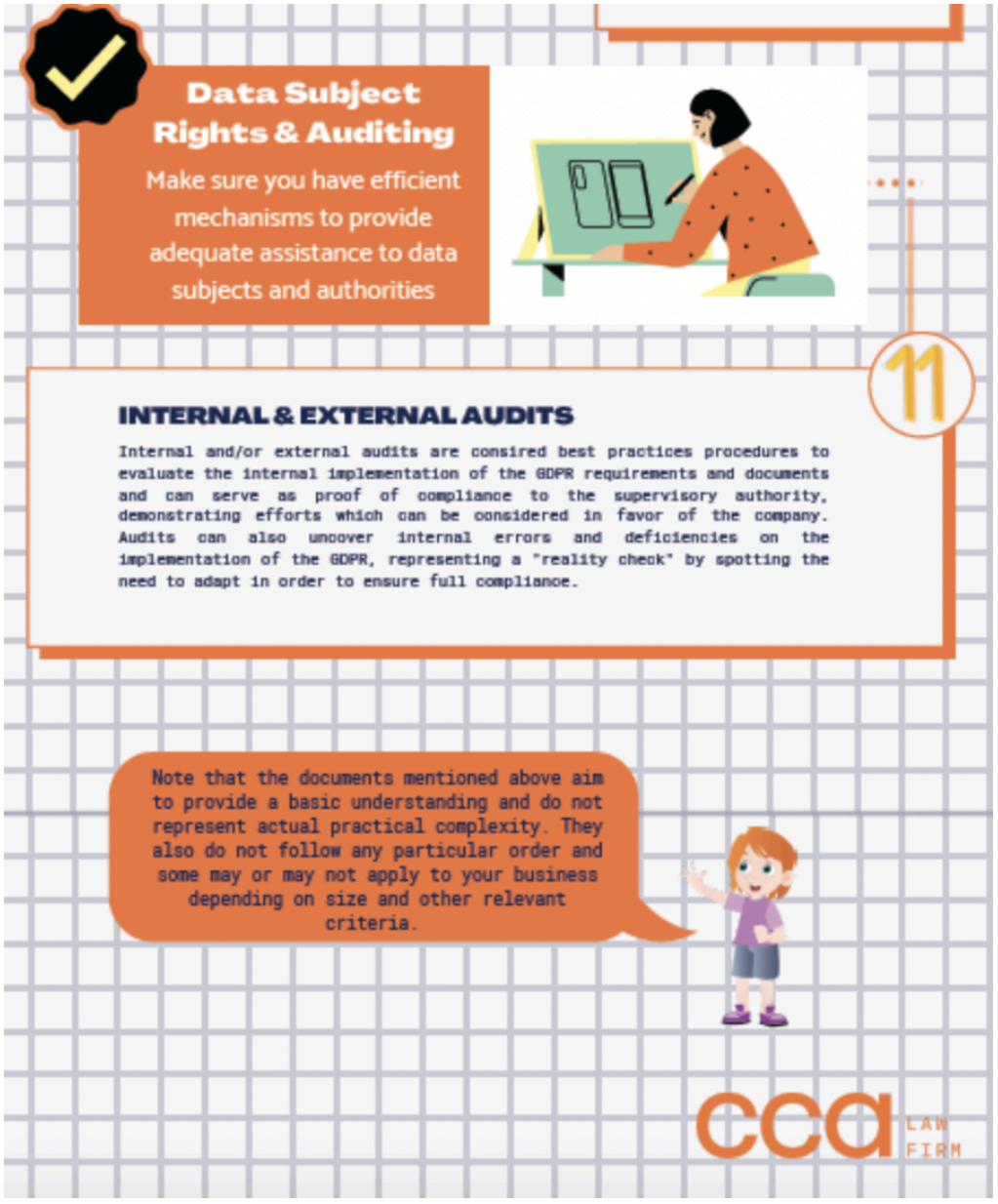
IV. Data privacy framework & culture

Developing a data privacy framework & culture is a multi layered & multidisciplinary process. It should involve the support of different teams, as well as the executive level; and the concretisation of subsequent measures.

The CCA Law Firm developed the Data Governance Roadmap below to exemplify and provide a basic understanding of what this process may entail:


Data Governance Roadmap
GDPR Compliance & Best Practices
Awareness, Trainning & Communication
Data Mapping & Gap Analysis
Analyse the data you process and identify the legal basis, international transfers and vulnerabilities
1
DATA MAPPING
Define what data shall be processed and the purpose of their processing
Define the category and the data flow of the processed data
Define who will have access to the data
identify the legal basis
2
RISK AND GAP ASSESSMENT
Assess the probabilities and consequences of potential risks, such as data protection and information security gaps covering also confidentiality, integrity and availability.
Policies & Contracts
Have privacy and cybersecurity internal and external policies & adequate contracts with third parties


3
PRIVACY NOTICE/ PRIVACY POLICY
Statements that propose how your organisation applies (and complies with) the GDPR's data processing guidelines.
These are either external (notice) or internal (policy) statements of a company that set out information regarding the data to be collected (privacy notice), or display information on how data is supposed to be managed as a whole (collected, stored, etc)- internally.
4
DATA PROCESSING AGREEMENT (DPA)
Agreement between a data controller (such as the main company) and a data processor (such as a third-party service provider) with the purpose of laying out the technical requirements and obligations for the controller and processor to follow when processing data.
5
JOINT CONTROLLERSHIP
Agreement for when two or more controllers jointly decide to determine the purposes and means of processing the same personal data (they have the same processing purposes or closely linked, complementary purposes)
Whilst the DPA regulates a relationship between a controller and a processor of data, a joint controllership splits the processing of data between two controllers.
6
INTERNATIONAL TRANSFER AGREEMENT AND SAFEGUARDS
Mandatory document if transferring personal data to a non-EU member state, unless adequacy decisions have been established for that state or model clauses have been agreed upon as your lawful ground for cross-border data transfers.
7
CYBERSECURITY & INCIDENT RESPONSE POLICY
Make sure to have a standard procedure that regulates the prevention and reaction to cybersecurity events.
Policy points might include:
• Detection and analyses
• Roles and Responsibilities
• Mitigation and Recovery
• Incident Communications
Risk Management & Assessments
Run assessments regularly and implement appropriate protocols in order to identify gaps and mitigate risks with auditable tracks.


Data Subject Rights & Auditing
Make sure you have efficient mechanisms to provide adequate assistance to data subjects and authorities
11
INTERNAL & EXTERNAL AUDITS
Internal and/or external audits are consired best practices procedures to evaluate the internal implementation of the GDPR requirements and documents and can serve as proof of compliance to the supervisory authority, demonstrating efforts which can be considered in favor of the company. Audits can also unoover internal errors and deficiencies on the implementation of the GDPR, representing a "reality check" by spotting the need to adapt in order to ensure full compliance.
Note that the documents mentioned above aim to provide a basic understanding and do not represent actual practical complexity. They also do not follow any particular order and some may or may not apply to your business depending on size and other relevant criteria.
cca LAW FIRM