Zint Technology Limited GDPR Compliance Statement

Background to GDPR:

The General Data Protection Regulation (GDPR) is an EU law on data protection and privacy for individuals within the European Union. Unlike a directive, it does not require national governments to pass any enabling legislation and so it is directly binding. As the UK is still a member of the EU, it affects all companies within the UK. Additionally, the UK government has stated that it will enforce almost identical legislation post-Brexit.

Some definitions:

GDPR will affect both controllers and processors. These terms have important definitions:

- A "controller" is an entity that decides the purpose and manner that personal data is used, or will be used.
- A "processor" is the person or group that processes the data on behalf of the controller. Processing is obtaining, recording, adapting or holding personal data

To give an example, in the case of a CRM tool like Salesforce (1), in which the end user of the Salesforce platform (2) would input information about their customers (3):

- The end user of the Salesforce platform (2) would be a "controller" of the personal data that they enter into the CRM about their customers.
- Salesforce (1) CRM platform would be a "processor" of the data that the end user inputs. Additionally, Salesforce would be a "controller" of the personal data of *their* customers (a different subset of individuals).
- The customers (3) of the end user of the Salesforce platform are defined as "data subjects".

"Personal data" is defined as any information relating to an identified or identifiable person, such as name, web cookie, image, date of birth and many more.

"Sensitive Personal Data" is defined under GDPR as "data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation." Zint neither controls nor processes any of this information.

Businesses need to have a legal reason to use the data of any EU-based "data subject". In the detailed regulation, we find 6 different justifications for why a company may process personal data:

- 6(1)(a) – Consent of the data subject

- 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- 6(1)(c) – Processing is necessary for compliance with a legal obligation
- 6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person
- 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- 6(1)(f) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

How this affects Zint:

Like many online companies, Zint deals with personal data.

Zint is an account-based sales platform that uses web-crawling and intelligent algorithms to profile UK businesses and associated information about them. Our users are able to identify UK-focussed legal-entities based upon several attributes to discover new business opportunities, grow their sales and do business more effectively.

Zint is a controller of the personal data of both our customers (i.e. the users of the Zint platform) and also the controller of personal data of key people associated with businesses we profile.

Zint compliance as a controller of the personal data of our customers:

- Lawful basis of processing: Zint has many existing users of the platform. In order to provide the service, Zint gathers data points on our users such as email addresses (to allow users to login and provide communications), location data (based upon IP addresses) and other information. These data points are required for legitimate business interests of Zint, which include being able to maximise the effectiveness of the Zint platform through user tracking, as well as allowing users to login to the site using their email, and to send billing information. We currently process this information in accordance with GDPR without consent but with legitimate business interest, that is to say, to allow our clients to access the platform and improve the effectiveness of Zint through monitoring of platform usage. Furthermore, Zint processes this data under 6(1)(b): “Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract” i.e. to provide our clients with access to our platform.

- Withdrawal of consent: Our users can withdraw their consent to our processing of their personal information at any time by getting in touch using the contact information on our website.
- Right to deletion: Our users can request that all their data be deleted from our records by getting in touch using the contact information on our website. We will respond within 30 days to any request.
- Subject Access Requests: Our users can request that we share with them a record of all personal information we have detailed on them by getting in touch using the contact information on our website. They may also request to see and verify the legitimacy of processing of such information using the same method.
- Data Modification: Our users can request that we change any personal details we have on record about them by getting in touch using the contact information on our website.

We use third party tools such as Stripe (for payments) and Mixpanel (for tracking of our users to measure effectiveness). We have received confirmation that they are doing everything in their power to become GDPR ready as "processors". You can find additional information on their compliance here:
https://support.stripe.com/questions/stripe-and-european-data-transfers#how-is-stripe-ensuring-the-adequate-protection-of-european-data-transfers
https://mixpanel.com/blog/2017/12/21/gdpr-mixpanel-readiness/

Zint as a controller of the personal data of businesses we profile:

Lawful basis of processing:

As well as business data points, such as company name, company phone number, product imports and exports etc. (which makes up the vast majority of information we gather), Zint also profiles key people associated with each business. This includes directors, secretaries and persons of significant control listed on the UK Company Register and we identify personal data such as name, address and month and year of birth.

To comply with GDPR, Zint must identify the lawful basis for processing of this information. The lawful basis is a legitimate business interest: we provide this information to provide our customers with a detailed picture of a UK business to facilitate them to discover new business opportunities, grow their sales and do business more effectively. For compliance with GDPR, this legitimate business interest must not outweigh or cause undue impact on the individual in question. In the case of Zint's profiling of such individuals within businesses, given that they already have the knowledge that their information will be placed in the public domain by virtue of being a company director/secretary/person of significant control, identifying these individuals in this way has no impact on that person.

To clarify this point further, currently the Registrar of Companies in the UK relies on the exemption from Paragraph 5 of Schedule 2 Part 1 in the Data Protection Act 2018 to make information on these individuals publicly available. Please refer to Companies House for further information:

https://www.gov.uk/government/organisations/companies-house/about/personal-information-charter

In this way, Zint is able to comply with GDPR through a legitimate business interest of helping our clients to make better business decisions whilst having no impact on the data subject (the director/secretary/person of significant control), given that their data must, by virtue of their position, be openly available and held in the public domain through the UK Companies Act. Zint regularly validates this information is still accurate in the UK Company Register and deletes or updates any information appropriately.

Withdrawal of consent: Individuals that we have identified through the UK Company Register can withdraw their consent to our processing of their personal information at any time by getting in touch using the contact information on our website.

Right to deletion: Individuals that we have identified through the UK Company Register can request that all their data be deleted from our records by getting in touch using the contact information on our website. We will respond within 30 days to any request.

Subject Access Requests: Individuals that we have identified through the UK Company Register can request that we share with them a record of all personal information we have detailed on them by getting in touch using the contact information on our website. They may also request to see and verify the legitimacy of processing of such information using the same method.

Data Modification: Individuals that we have identified through the UK Company Register can request that we change any personal details we have on record about them by getting in touch using the contact information on our website.

Zint general GDPR compliance:

- Data Protection Officer: Fraser Atkins (also a company director) has been appointed as the data protection officer and is responsible for overseeing data protection.
- Security Measures: The following security measures are in place:
    - All sensitive data sent to and from Zint servers is processed in an encrypted manner via e.g. HTTPS, SSL etc.

- Zint servers are regularly updated to the latest operating system to ensure security and minimise the risk of exposure to vulnerabilities.
- The use of physical, external storage devices is minimised.
- When the office is left empty for any reasonable period, employees are trained to lock doorways and windows to prevent access to any physical items or data on machines etc.
- Employees and contractors of Zint are trained in the importance of secure passwords.
- Personal data we hold is regularly reviewed and any redundant (with the exception of backups) or obsolete data is deleted.