Data Privacy and GDPR Compliance Policy

1. INTRODUCTION

1.1 As a global non-profit membership organisation, the Responsible Business Alliance ("**RBA**") has a responsibility to ensure that it uses personal data in accordance with the law. As such RBA has developed this Data Privacy Policy ("**Policy**"). Everyone in RBA is accountable for upholding the Policy's requirements.

1.2 RBA is committed to handling personal data responsibly and in compliance with applicable data privacy laws worldwide. This Policy is designed to provide a global baseline with respect to the protection of personal data. RBA recognises that in some jurisdictions certain laws may impose additional requirements. RBA will handle personal data in accordance with all such applicable laws.

1.3 This Policy covers our use of personal data, for instance about [members, subscribers to our newsletters, customers, students (e.g. of the eLearning academy, employees, contractors and vendors] (for more detail see section 2.6). We need to comply with the Rules set out in this Policy about how we use personal data. No one is exempt from compliance with these Rules.

1.4 This Policy does not form part of any employee or volunteer contract and may be amended at any time. You will be notified of any significant changes.

YOU ARE REQUIRED TO FAMILIARISE YOUSELF WITH THIS POLICY.

2. BACKGROUND

2.1 What is data privacy law?

Data privacy (or data protection) law gives people the right to control how their 'personal data' (any information that relates to them, such as name, contact details, allegations of criminal activity, preferences etc.) is used. It also places obligations on organisations that use personal data.

Personal data is interpreted as a broad concept by European data protection authorities and the courts. So information may be personal data even if a person's name is not associated with the information.

Since 25 May 2018, all countries in the European Union are subject to the General Data Protection Regulation (GDPR), which replaces EU Directive 95/46/EC, and existing local law will be substantially repealed.

2.2 How does data privacy law affect RBA?

RBA holds personal data on various categories of individual (see section 2.6 below).

2.3 **What are we doing about it?**

RBA treats compliance with its obligations very seriously. We wish to maintain the highest possible standards of compliance to ensure in particular that individuals are properly protected and that our internal procedures are designed to ensure compliance. We have developed this Policy to ensure that the personal data we collect and use is done so in accordance with applicable data privacy laws.

2.4 **What are the consequences if we get it wrong?**

Getting it wrong is serious for RBA. It could also lead to complaints from individuals, compensation claims, fines from regulators and negative publicity for RBA. If you deliberately fail to observe this Policy we will consider disciplinary action against you.

2.5 **Why is this policy important for RBA?**

It is vital that those working as part of RBA observe this Policy because the collection and use of personal data is part of our everyday business. We must ensure that we use the information we hold on our customers, employees etc. in accordance with the law.

2.6 **What types of personal data does RBA collect?**

RBA collects personal data regarding:

(a) [Employees and contractors (and applications for those positions) in connection with their (potential) role within RBA including contact details, resume, professional development, personnel file, benefits, compensation etc.

(b) Customers and members (and their personnel) in connection with the services we provide to them;

(c) Individuals working at organisations we audit;

(d) Subscribers to our newsletters;

(e) Students (e.g. of the eLearning academy);

(f) Vendor personnel for the management of the vendor relationship, including our vendor partner members.]

(g) Suppliers of Members

2.7 **When should you collect and use personal data?**

You must only collect and use personal data in compliance with this Policy including the Rules set out below.

2.8 **How does this Policy relate to other policies within RBA?**

This Policy sits alongside RBA's *[Information Technology Security Policy, which includes the RBA Written Information Security Policy, Vendor Management Policy, Data*

Classification and Handling Policy, User Access Management Policy, Incident Response Plan, and Secure Configuration and Hardening Standards.]]

2.9 **Want more information?**

If you want more information about the data privacy policis above and how the rules affect RBA please contact *kanderson@responsiblebusiness.org*

3. THE RULES

3.1 Ensuring Transparency

The Rule: We must be transparent about the personal data that we hold on individuals including describing the purposes for which we use personal data.

3.1.1 Understanding the Rule

Being open and transparent in the way we use and share personal data is an important step to demonstrate good data privacy practices. As an example, we are subject to this requirement in how we use personal data on members' personnel and employees – as such members and employees must be told when we use their personal data.

There may be limited circumstances where we do not have to comply with the transparency requirement but you should check with [the RBA IT Director] before you proceed without ensuring transparency.

3.1.2 Practical Steps

Our members and employees must be provided with information about fair processing where we collect and use personal data about them. All employment contracts and our Employee Handbook must include suitable wording notifying the individual of how we will use their information.

If we offer individuals the opportunity to opt-out from or opt-in to receiving marketing or other uses of personal data, or the opportunity to access and correct personal data, such opportunities must be clear, conspicuous and easy to use.

3.2 Collecting and using personal data for a lawful purpose only

The Rule: We must only collect and use the minimum amount of personal data which is necessary for one or more legitimate business purpose which must be lawful and justifiable

3.2.1 Understanding the Rule

We must only collect and use personal data (i) where it is relevant to our business purposes (e.g. a Human Resource (HR) purpose or to supply membership services), (ii) where we can rely on a lawful basis (or bases – see paragraph 3.2.2 below), (iii) where the purposes for which the personal data are used are identified in the data privacy notice provided to individuals (usually at the point where personal data is collected), and (iv) where the use of the personal data is within the individual's reasonable expectations.

We must also comply with any local laws.

3.2.2 Practical Steps

When collecting personal data from individuals, we must ensure that the privacy notice made available to those individuals contains all of the purposes for which the personal data may be used.

In addition, when collecting personal data, we must only collect those details which are necessary for the purposes for which that personal data is being obtained. Any use of personal data must be for the identified purposes and any different or new purposes should have a lawful basis. Personal data that is not necessary for a business purpose should not be collected or accessed. You must not use any personal data accessed through your role for any private interest.

Can we rely on consent?

In some circumstances (though not always), use of personal data requires us to obtain the relevant individual's consent to the collection and use of their personal data. For instance, consent is often required in order to send marketing to individuals. But consent is not always an appropriate ground to rely on.

Consent is only valid if it is specific and informed so we must provide clear and unambiguous information on the purposes for which the personal data will be used when we collect consent. Consent must also be genuine and freely given so individuals must have a real choice about whether to provide their consent and must not be under pressure to consent.

It is important that we obtain documented evidence of the provision of consent (e.g. in writing or via the use of an opt-in procedure). Our use of personal data must not fall outside the purposes set out in the consent declaration and should not be used for different purposes.

Relying on explicit consent

In order to use certain types of personal data – known as special categories of data – we may need to obtain explicit consent from individuals. Special categories of data require additional protection. Special categories of data are data revealing racial of ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or sex life or sexual orientation.

Explicit consent can be effectively obtained where an individual is presented with a proposal to either agree or disagree to a particular use of his or her personal data and actively responds to that proposal, either orally or in writing (which could be a wet ink signature on a piece of paper, or electronically through the use of an electronic signature, clicking icons or sending confirmatory emails). But the need for explicit consent means it is not possible to construe implied consent through a person's actions.

What about the legitimate interest lawful basis?

EU data protection law specifically allows processing of personal data where an organisation can rely on the legitimate interest lawful basis. It is not always obvious what

this means and when we can rely on it. However, if we wish to rely on the legitimate interest lawful basis we need to be able to satisfy the test below:

1. We must identify a legitimate interest for using personal data for a particular purpose. It could be our legitimate interest as an organisation or a third party's legitimate interest. For example: combating fraud, protecting network security, suppressing details on our marketing lists, direct marketing by mail etc.
2. We must consider whether the processing of the personal data is necessary for satisfying that identified legitimate interest. In other words, could we further the same interest without processing the personal data or could another less intrusive way be used.
3. We must balance the legitimate interest we have identified with the rights and freedoms of individuals whose personal data we will process. Are we sure that the rights and freedoms of individuals do not override the identified legitimate interest? In considering how to balance the different factors we must consider the nature of the various interests, the impact of the processing on individuals and on us (including how intrusive it is), as well as the safeguards that we will put in place to reduce the risk to individuals.

We must always document the assessment we have carried out when considering the legitimate interest basis for processing personal data.

3.3 Privacy Impact Assessments

The Rule: Where the collection and use of personal data is likely to result in significant risks for the rights and freedoms of individuals, we must carry out an assessment into the impact of the proposed collection and use on individuals

3.3.1 Understanding the Rule

Where we intend to use personal data in a more intrusive way we must carry out an initial assessment to consider whether the use is justified. Carrying out a PIA (also known as a Data Protection Impact Assessment) helps us identify and minimise the privacy risks associated with the use of personal data. We may be able to rely on one PIA for similar processing. Additionally if we intend to collect and use personal data in a way that could result in discrimination, identity theft, fraud or financial loss, we must make an initial 'screening' assessment of whether or not we need to carry out a full PIA.

As part of the PIA, we must evaluate the origin, nature, particularity and severity of any risk to the privacy of individuals.

3.3.2 Practical Steps

[The RBA Human Resources contact or IT Director] should be informed of any such screening process. You must not proceed with the collection and use of personal data until you have provided the outcome of that screening to the [The RBA Human Resources contact or IT Director] and received guidance on whether a full PIA is required or not. [The RBA IT Director] is entitled to ask further questions and will work with you to mitigate any potential risks to the privacy of individuals.

In certain circumstances, we may be required to consult with the local data protection authority about the proposed use of personal data.

3.4 Ensuring data quality

The Rule: We must keep personal data accurate and up to date

3.4.1 Understanding the Rule

Processing inaccurate information can be harmful to individuals and the RBA. The main way of ensuring that personal data is kept accurate and up to date is by ensuring that the sources we use to obtain personal data are reliable.

Individuals should be actively encouraged to inform us when their personal data changes.

We must track when information was last updated.

3.4.2 Practical Steps

In the employment context, employees should be actively encouraged to update their details (e.g. change of address) and HR will also perform routine updates.

To practically ensure that personal data is accurate, it should generally be collected directly from individuals affected. All member contacts should be actively encouraged to update their contact details by inviting them, when communication occurs, to notify us of any changes in their personal data.

3.5 Retaining and disposing of data

The Rule: We must keep personal data only for as long as is necessary for a specific business purpose and ensure it is securely disposed of

3.5.1 Understanding the Rule

Any personal data must only be kept where there is a business or legal need to do so. When we dispose of personal data, this must be done in a secure manner.

Laws, regulations or contractual obligations may require that certain personal data be retained for a specified length of time, and it may also be prudent to keep certain personal data for a specific period so that we are able to defend properly any legal claims or manage an ongoing business relationship, such as that with our members or our vendors.

Documents (including paper and electronic versions and email) containing personal data must not be kept indefinitely and must always be securely deleted and destroyed once they have become obsolete or when that personal data is no longer required. Personal data must not be retained simply on the basis that it might come in useful one day without any clear view of when or why.

3.5.2 Practical Steps

We must follow all internal data retention policies in relation to:

- The key applicable retention requirements from both a business and (where applicable) legal perspective
- Procedures for ensuring that personal data is retained when needed and securely destroyed afterwards
- The process for suspending the destruction of documents in situations relating to pending, threatened or reasonably likely litigation, regulatory or governmental investigations
- The responsibilities of those involved in retention activities relating to personal data.

3.6 Honouring individuals' rights

The Rule: We must always be receptive to any queries, requests or complaints made by individuals in connection with their personal data and adhere to our Individual Rights Request Policy

3.6.1 Understanding the Rule

We will reply to queries and complaints, usually free of charge to the individual, within a reasonable time and to the extent reasonably possible concerning the processing of personal data by us. We consider that the most important of all data privacy rights is the ability of individuals to access the personal data that we hold about them and to expect that it will be corrected if it is inaccurate.

Under the GDPR, individuals are entitled (by making a request) to be supplied with a copy of any personal data held about them (including both electronic and paper records). Individuals are also entitled to know the logic involved in decisions made about them.

An individual also has the right to seek erasure of their personal data and to request that we provide their personal data to them in a structured, commonly used and machine-readable format.

3.6.2 Practical Steps

Where we receive a request from an individual exercising their legal right to access, object to or modify their personal data, we must follow the steps set out in our Individual Request Response Policy. Our procedure provides a description of events designed to ensure that valid requests are processed in line with applicable legislation.

If a valid request concerns a change in that individual's personal data, such information must be rectified or updated, if appropriate to do so.

3.7 Taking appropriate security measures

The Rule: We must always take appropriate technical and organisational security

measures to protect personal data

3.7.1 Understanding the Rule

Personal data must be kept secure. Technical, organisational, physical and administrative security measures (both computer system and non-computer system related steps) are necessary to prevent the unauthorised or unlawful processing or disclosure of personal data, and the accidental loss, destruction of, or damage to personal data.

When considering what level of security to implement in each particular case, a number of factors must be taken into account including:

- The state of technological development
- The cost of implementing any measures
- The harm that might result from a breach of security
- The nature of the information to be protected – for example special categories of data require greater security

In certain circumstances, where we fail to take appropriate security measures, we may suffer a data security breach and may then be required to notify a local regulator and the individuals affected. If we fail to comply with these reporting requirements, we can receive a fine.

3.7.2 Practical Steps

We must monitor the level of security applied to personal data and take into account current standards and practices. In particular, we must observe the requirements set out in our IT Security Policy and any other requirements set out under the applicable local data privacy laws.

If you become suspicious or are actually aware of any data security breach, you must immediately report the breach to the [RBA IT Director]. When we become aware of a breach we can take protective measures that can effectively mitigate the consequences of the breach.

3.8 Adopting Privacy by Design

The Rule: We must adopt privacy by design and privacy by default in all systems, databases, tools and features we build to collect and use personal data

3.8.1 Understanding the Rule

Taking account of the particular circumstances of the data collection and use, the cost of implementing measures and the risks to individuals, we must implement measures (such as pseudonymisation) that reflect data protection principles when we design systems, databases, tools and features to process personal data.

3.8.2 Practical Steps

We must ensure that any privacy settings are by default set to the most privacy protective setting. We must ensure that the minimal amount of personal data is collected and used through our technology.

As far as possible we should employ pseudonymised datasets to reduce risk to individuals' privacy.

3.9 Using subcontractors/ vendors

The Rule: We must ensure that providers of services to us also adopt appropriate and equivalent security measures in relation to any personal data they process on the RBA's behalf

3.9.1 Understanding the Rule

Under EU data protection law, where a provider of a service has access to our personal data (e.g. as a payroll provider) we must impose strict contractual obligations limiting the purposes and ways our personal data may be used and ensuring appropriate security of that personal data. This includes vendors who host personal data on our behalf.

3.9.2 Practical Steps

We must always complete a vendor due diligence questionnaire (or otherwise carry out appropriate due diligence) which considers the vendor's security measures for processing personal data before we engage a vendor.

We must always enter into a written contract with any vendor that deals with personal data on our behalf. All contracts with vendors should include our standard contractual provisions. Consult with [the Legal Team] to ensure your contracts are up to date with the most recent data privacy provisions.

3.10 Disclosing to third parties

The Rule: We must only disclose personal data to third parties where we have the consent of the individual, where required by law or where the third party is a subcontractor/ vendor that has a need to know the information to perform its services and has entered into a contract with us containing the appropriate data privacy and security provisions

3.10.1 Understanding the Rule

At times, we may disclose personal data to Vendors, contractors, service providers and other selected third parties.

Prior to disclosing personal data to these parties, we will take reasonable steps to ensure that: (i) the disclosure of personal data is consistent with our IT Security Policy; (ii) the recipient of such information is identified; and (iii) where appropriate or required by law, the

third party is contractually committed to complying with this Data Privacy Policy and/ or our instructions concerning the use of personal data as well as implementing appropriate security measures to protect personal data, limiting further use of personal data, and complying with applicable laws.

In certain circumstances, we may be required to disclose personal data to third parties when required by law, when necessary to protect our or others' legal rights, or in an emergency situation where the health or security of an individual is endangered. Prior to such disclosures, we must take steps to confirm that the personal data is disclosed only to authorized parties and that the disclosure is in accordance with this Policy, other applicable RBA policies and/ or operating procedures, and applicable law.

3.10.2 Practical Steps

If you receive a request from a third party asking you to disclose personal data to them, you should contact the RBA IT Director] unless it is a business as usual request i.e. it is the type of request that you typically receive in connection with your role which you regularly comply with and involves no significant disclosure of personal data. For example, providing the names of those on the management board of the RBA.

Any disclosures must be in accordance with RBA's IT Security Policies **Ensuring adequate protection for international transfers**

The Rule: International transfers of personal data are subject to certain legal restrictions and therefore we must ensure that all transfers are subject to appropriate safeguards through putting contracts or internal policies in place

3.10.3 Understanding the Rule

The law may restrict international transfers of personal data to countries that do not ensure an 'adequate' level of data protection. There is then a requirement to implement appropriate safeguards. Appropriate safeguards can be achieved through a number of mechanisms such as contracts or internal policies. All cross-border transfers of personal data within the RBA need to meet this rule (for example, personal data passing between our EU-based technical experts and our US offices). International transfers of personal data outside the RBA are not allowed without appropriate steps being taken, such as contractual clauses which will protect the personal data that is being transferred.

3.10.4 Practical Steps

We must not transfer any personal data across borders without checking whether a legal restriction is in place. This includes if you are dealing with service providers or third parties based in another country and we are transferring personal data to them or allowing them to remotely access our systems/ data. When in doubt about the lawfulness of any transfer, please contact the [Legal Team] and the RBA IT Director] on how to proceed.

3.11 **Safeguarding the use of special categories of data**

The Rule: We must only use special categories of data if it is absolutely necessary for

us to use it and, in certain circumstances, we should obtain explicit consent from individuals to use their special categories of data.

3.11.1 Understanding the Rule

Special categories of data are information revealing an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, processing of genetic data or biometric data (for the purpose of uniquely identifying an individual), health and sex life or sexual orientation. Since this information is more intrusive, we must only use it where absolutely necessary and usually with the explicit consent of the individual affected.

The proposed collection and use of special categories of data should be heavily scrutinized and challenged before proceeding. The consent from individuals to our use of their special categories of data must be genuine and freely given.

We can only hold and make available special categories of data on an individual without their explicit consent if we have another lawful basis under applicable law. This may be the case, for example, where we hold information about an employee's health where this is necessary to exercise any obligation conferred by law on us in connection with employment.

3.11.2 Practical Steps

- We must always assess whether special categories of data are essential for the proposed use – why do we need it?
- We must only collect special categories of data when it is absolutely necessary in the context of our business – why do we need it?
- Application (or other) forms used to collect special categories of data must include suitable and explicit wording expressing the individual's consent.
- Consent must be demonstrable. Therefore, when it is collected verbally it must be recorded in such a form as to prove that the requisite information was provided to the individual and their response was able to be verified.
- Where consent is not relied upon, we must take steps to ensure that there is another lawful basis under applicable law for the collection and use of such information.
- The RBA IT Director] should be informed of any planned significant use of special categories of data to verify the legitimacy of such use. The RBA IT Director] is entitled to ask further questions and will work with you to mitigate any potential risks in this regard. In certain circumstances, we may be required to consult with the local data protection authority about the proposed use of such special categories of data.

3.12 Legitimising direct marketing

The Rule: We must obtain consent from individuals to use their details for direct marketing where the law requires. We must always allow customers to opt out of receiving marketing information

3.12.1 Understanding the Rule

In the context of electronic marketing (e.g. by email or SMS), the default position is that we must obtain prior consent from individuals before sending marketing to them.

One of the key data protection rights is that individuals have the right to object to the use of their personal data for direct marketing purposes and we must always notify individuals of their right.

3.12.2 Practical Steps

We must ensure we collect valid consent from individuals before sending them e-marketing if consent is required by law.

We must ensure that the privacy notice made available when personal data is collected includes the relevant opt-out mechanisms regarding marketing communications.

3.13 Honouring opt-outs

The Rule: We must always suppress from marketing initiatives the personal data of individuals who have opted-out of receiving marketing information.

3.13.1 Understanding the Rule

It is essential that individuals' choices are accurately identified when direct marketing campaigns are carried out. A failure to comply with an individual's opt-out choice (e.g. by sending a mailing to an individual who has previously indicated to us that he or she does not wish to receive mailings) is likely to lead to complaints from the individual and possible scrutiny or enforcement action being taken by a data protection regulator.

3.13.2 Practical Steps

Where we are responsible for a direct marketing campaign about the RBA and we are using information collected by the RBA, we must take all necessary steps to prevent the sending of marketing materials to individuals who have opted-out.

4. COMPLYING WITH THE RULES

4.1 Why is it important that I comply with the Rules?

It is important that everyone within the RBA complies with the Rules since we are all responsible for data privacy compliance. A failure to comply with the Rules could expose us to regulatory and/ or legal action which could mean the payment of compensation, damages and/ or fines as well as other remedies.

4.2 What happens if I breach a Rule?

If you breach a Rule, even inadvertently, you must immediately inform the [RBA IT Director] even if you are not certain whether the breach is serious. You should always voluntarily tell

us of any serious breaches since we will consider any deliberate cover up or attempts to mislead us about a breach as a serious disciplinary matter.

While we would always seek to work through any breach incident with you in order for you to understand the ramifications of your actions or omissions and continue to work on the same basis, regrettably, in some circumstances, we may have to commence disciplinary action against you if the breach is of a particularly damaging nature and, ultimately, we may have to terminate your contract.

Additionally you should note that knowingly or recklessly obtaining or disclosing personal data may be a criminal offence and could also result in damages or compensation claims against you.

4.3 Auditing compliance with the Rules

We will conduct periodic audits to ensure compliance with the Rules. All employees must participate with such audits and any outcomes, including remediation plans.

4.4 Are there exceptions to compliance with the Rules?

In limited circumstances, such as co-operating in criminal or other government investigations or inquiries, it may be appropriate for RBA to obtain an exception from compliance with part or all of these Rules. All such exception requests must be approved by the [RBA Chief Operating Officer or Executive Director].

4.5 Who enforces data protection law?

Data protection law is usually enforced by data protection regulators and the courts. In the UK, the data protection regulator is the Information Commissioner's Office. In Sweden, the data protection regulator is the Swiss Data Protection Authority (or Datainspektionen). These authorities have powers to serve notices on us and to conduct assessments of our operations. Ultimately and for the most serious breaches, we can be fined.

5. TRAINING ON THE RULES

We require all relevant employees and contractors to receive training on the Rules.

Further information is available here *[insert details].*

6. IMPLEMENTATION

This Policy is effective from *[January 01, 2019]* and is next due for review on [July 01, 2019] or sooner if there are significant changes to law or regulation, or to internal policy or processes, before that date.

7. MAINTENANCE AND CONTACT

The review and maintenance of this Policy is the responsibility of the [RBA IT Director]. Queries and feedback should be directed to the [RBA IT Director] at: *kanderson@responsiblebusiness.org].*

[January 01, 2019]

Version 0.1