Principles

For commercial, ethical and legal reasons we wish to operate to the highest professional standards and endeavour to do so at all times. Our policy is to comply fully with the General Data Protection Regulations 2016/679 and the Privacy and Electronic Communications Regulations and all other relevant laws and regulations.

Legal principles

We will ensure that all personal data is :

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Legitimate reasons for holding and processing data

And we will only process personal data if one or more of the following applies:

(a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for us to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Legitimate interest assessments

When assessing legitimate interests we will consider:

Our interest

- Why do we want to process the data – what are we trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if we couldn't go ahead?
- Would wer use of the data be unethical or unlawful in any way?

The need to do so

- Does this processing actually help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

Balanced against the impact

- What is the nature of our relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect we to use their data in this way?
- Are we happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual?
- How big an impact might it have on them?
- Are we processing children's data?
- Are any of the individuals vulnerable in any other way?
- Can we adopt any safeguards to minimise the impact?
- Can we offer an opt-out?

Practice

The following section sets out how we apply the principles of a policy that is commercial, legal and ethical to our business. It explains how we balance legitimate interest and privacy and recognising that there are differences of view as to what is reasonable, how we address those individual differences of view.

Almost all of the data processing we do is for purposes (a) and (b) when dealing with employees, clients, suppliers and other partners. Purpose (f) applies in almost every other case. We have a legitimate interest in building new relationships that enable us to sustain the business.

Our policy is to process data only in ways that are reasonable and with respect for privacy. We do not envisage any circumstances where that would not be the case and yet a compelling justification might exist, although if such a situation did exist we would by definition take the compelling action.

The main, section of our policy provides details of the specific types of processing we do and for what types of data and why.

By setting out openly and clearly our policy, and making it widely available via our website, emails and other places, we not only communicate how we endeavour to balance our legitimate interest against people's rights and interests, we also address varying perceptions as to what is reasonable.

By giving people the opportunity to review our policy and to inform us if they disagree we can take into account their individual view. Our policy is that if an individual informs us of their view as to what balance is reasonable for them, we will, wherever possible and practical, adjust our records and our processing to align our actions for them and their data with their individual view as to what is reasonable.

Detail

Who are we?

This policy applies to Hardybee Ltd, trading as MD2MD and otherwise. Hardybee Ltd is the data controller. The data, this policy, and its implementation is managed by our Managing Director who also acts as our Data protection officer.

Our policy is to ensure that all staff understand and comply with this policy. All staff have been trained on the implementation of the policy and all new staff are provided with the policy, and briefed on its application in practice within our business. They are encouraged to raise any concerns about its practical application with the Data protection officer.

Who do we hold data on and for what legitimate interest?

Our policy is not to hold data on members of the general public. We only hold data on individuals who hold or have held a role in a business and our legitimate interest is as a consequence of that role.

We hold and process such personal data where the business has a commercial relationship with us. This includes clients, staff and suppliers.

Our legitimate interest in doing so is primarily to enable us to deliver our service efficiently to them. A secondary interest is to monitor, develop and enhance our service. It is reasonable to do so as we could not deliver our service without doing so and we believe they would expect us to process data in this way.

We also hold and process similar personal data where we believe the business might wish to have a commercial relationship with us.

Our legitimate interest in processing this data is to identify, develop relationships with, and if appropriate form commercial relationships with new clients that have needs we can help them address through our services. To do so we collate information that enables us to do so only when appropriate, and in an appropriate and personalised manner. This information is collated primarily from the public domain online with supporting information from individual conversations,

As these are potential or developing relationships, not all contacts will be aware of us at the when we first identify them as potentially having a need we can address. It is therefore not possible to say they would expect us to be processing data about them. Most reasonable people (as cited in case law as the man on the Clapham Omnibus) would however expect a business to be endeavouring to identify new clients and we have a legitimate interest in so doing and therefore such activity can be reasonable if balanced against the rights of individual to privacy.

It is worth noting here that our commercial interest is entirely in line with data protection principles in that we do not wish to incur the cost of communication with anyone who does not wish us to be communicating with them. A key reason for investing in our main CRM database system where almost all our contact information is held is to enable us to contact only appropriate individuals in an appropriate way with information appropriate to them in their business role.

The following paragraphs set out how we endeavour to be better than most at achieving the right balance given the lack of pre-awareness:

- We endeavour to identify only relevant people. This is quite simple for us as our service is exclusively for business leaders and their senior team, where business includes third and public sector entities. To be able to record relevance though may mean capturing the information that others are not relevant.
- We endeavour to make contact in a manner that is as personalised and appropriate manner as we can practically and commercially achieve. Indeed this is a key reason for collating the information we do.
- We respect their right to tell us (implicitly or explicitly) how they want their data to be handled and take whatever action is appropriate in light of any such requests. We do so through formal subscribe and unsubscribe methods.
- We also encourage such feedback informally. We consciously endeavour to proactively encourage contacts to tell us whether and how they want us to communicate with them through simple comments like “Is it ok to keep in touch?” and “If you are not interested, please say” and “when would it be appropriate to talk again”.

We do not treat contacts within legal entities as different to sole traders and unincorporated businesses as it is our policy is to engage only with individuals in their business role and with information we know or believe is specifically relevant to them in that role.

What systems do we use to hold data?

The majority of personal data we hold is held on our CRM (Customer relationship management) database system. We use this as the primary reference point for all personal information. It is a central record of all the information we have about contacts, including but not limited to past, current and prospective staff, clients and suppliers. Holding this data enables us to ensure we contact them appropriately. It is searchable by individual.

A subset of our CRM system data is synchronised with our email and newsletter systems to enable email contact.

We also have an accounts system. This primarily contains information about client and supplier businesses. It contains very limited personal information solely related to contacts involved in managing our financial relationship with those businesses.

In order to operate our business we use in a limited way a number of smaller systems. We have an older CRM system we are phasing out and a number of WORD documents and EXCEL spreadsheets with extracted information relevant to the activity we are managing such as attendee lists and feedback analyses. These are not indexed or filed by person.

We do not hold personal records on paper and have no manual files for personal information.

What data do we hold?

Our CRM contains the structured (such as name, job title, email address, phone number and location) information we need to contact individuals within a business, records of communications with them by email, telephone, face to face and through social media. It also contains background information about them and their business that allows us to engage with them as an individual business person as is our intent. That information is gained through personal interaction and knowledge and public domain sources such as the media and online searches and websites.

Our policy is to only record personal data in an ethical and professional manner. We would expect that all data recorded is fair and that almost all data recorded would be data that the individual is entirely comfortable with us having on record. In the exceptional cases where the individual might not be fully comfortable with our record, our policy is only to record such information in a professional and commercial way that would be viewed as reasonable by the wider public. Eg This person / business didn't pay their invoice on time.

How do we use data?

First and foremost, we use your personal data to provide you with any services you've requested, and to manage our relationship with you. We also use your personal data for other purposes, which may include the following:

To communicate with you. This may include providing you with information, and requesting information, especially about our events and membership and related marketing communications. Our policy is always to respect your expressed marketing preferences unless we are obliged by law to act otherwise

To protect: So that we can detect and prevent any fraudulent or malicious activity, and make sure that everyone is using our websites and services fairly and in accordance with our terms of use.

To market to you: In addition to sending you marketing communications, we may also use your personal data to display targeted advertising to you online – through our own websites and services or through third party websites and their platforms.

To analyse, aggregate and report: We may use the personal data we collect about you and other users of our websites and services (whether obtained directly or from third parties) to produce aggregated and anonymised analytics and reports, which we may share publicly or with third parties.

Do we hold sensitive personal data

No. Our policy is to avoid holding information on racial or ethnic origin, political opinions, religious beliefs, trade union membership, health and information on sex life, sexual orientation or genetic, biometric or medical data except where holding such data is necessary for the safe and effective provision of our business (eg Details of special dietary requirements, details of person to contact in an emergency).

Photographs, Videos, Sound recordings and Quotes

We and our partners may, at times take photographs, videos and sound recordings at events and may also ask participants to participate or provide quotes about the event. We reserve the right, subject to the protections following, to use such recordings for promotional and other purposes in relation to our business.

We protect the privacy of participants through a number of further detailed policies. Firstly, no individual or business will be named in relation to that recording unless that has been individually agreed either explicitly or through clear context such as requesting a quote or filming a testimonial. Secondly such recordings will be done so openly, not in secret and we will endeavour to draw attention to the recording through appropriate notices. Finally, given this openness we will respect the privacy of anyone who informs that they do NOT wish to be included with or without identification.

Where are our systems (and data) located?

We do not have any internal storage servers. Our data is all held on individually managed PCs and mainstream proprietary global cloud solutions.

Individually managed PCs are all protected by passwords and by physical proximity to their user.

We access the mainstream proprietary global cloud solutions through the internet. It is fundamental to the nature of the internet that we are, like everyone else, unable to control the routing of that data. We do however protect that data through using HTTPS encryption. Similarly we cannot know for the proprietary cloud products we use precisely where the data is held at any moment in time and under what security conditions. They are though services provided by large global firms to large numbers of businesses in the UK and so judge it is reasonable to rely upon them as data processsors conforming to all legal requirements necessary to trade in the UK.

Who do we share data with?

Although we regard data as an asset of the business we never sell data for use outside the business.

We only share data as required by law and with partners and suppliers as required to enable them to work with or for us in promoting the business. Where we feel it is of value to BOTH parties we occasionally introduce contacts to each other by email and provide a minimal context for the introduction. We do not normally share phone number information as contacts can disclose that by email if they wish.

The only exception is that as our core purpose is to facilitate business leader to business leader engagement and our members have joined us for that purpose we will positively and proactively connect members and past members with each other at every practical opportunity and through every practical route.

Where does our data come from?

The data we use may have been provided by you directly, our systems may have collected it automatically through our website, social media or otherwise, or it may have been provided by third party partners.

Information you provide to us directly: When we make personal contact by email, phone or face to face, you may provide personal data to us. For example, you may provide a business card, connect or follow us on social media, fill in information online or respond to an email or phone call. If you don't want to provide us with personal data, you don't have to, but it might mean you can't use join or use some of our events or services.

Information we collect automatically: We collect some information about you automatically when you visit our websites or use our services, like your IP address and device type. We also collect information when you navigate through our websites and services, including what pages you looked at and what links you clicked on. This information is useful for us as it helps us get a better understanding of how you're using our websites and services so that we can continue to provide the best experience possible (e.g., by personalising the content you see). Some of this information is collected using cookies and similar tracking technologies.

Information we get from third parties: The majority of information we collect, we collect directly from you. Sometimes we might collect personal data about you from other sources, such as publicly available materials or trusted third parties like our marketing and research partners. We use this information to supplement the personal data we already hold about you, in order to better inform, personalise and improve our services, and to validate the personal data you provide.

What third parties do we work with?

We utilise a range of widely available standard digital services and appoint digital marketing agents to conduct marketing activity on our behalf. The systems used by these providers may sometimes contain elements of data about you. Our primary providers, include but are not limited to:

- Google. Primarily their Office suite, cloud services and associated tools.
- Microsoft: Primarily their Office suite, some cloud service and their LinkedIn platform.
- ZoHo: Primarily their CRM and some related applications. You can read their GDPR policy here: https://www.zoho.com/gdpr.html and contact them here: legal@zohocorp.com.
- Linkmatch. A service provided by LOGICAL HABITS OÜ. You can contact them and view their privacy policy here: https://linkmatch.net/privacy and you can find their GDPR statement here/ https://linkmatch.net/blog/how-linkmatch-is-complying-with-the-gdpr/ You can contact them here: team@linkmatch.net.
- Prospect Global Ltd (trading as SoPro) Reg. UK Co. 09648733. You can contact SoPro and view their privacy policy herehttp:/sopro.io. SoPro are registered with the ICO Reg: Z123456 their Data Protection Officer can be emailed at: dpo@sopro.io.

When do we delete data

If we become aware a business leader or other contact has left, retired or is no longer relevant to us we mark their contact status to reflect that or as simply Do not contact and we don't contact them again. We delete records when we have no further need to use or analyse it and when we don't need the record to avoid accidental contact. Our policy to avoid accidental contact is to retain the email address information whilst marking records as do not contact and setting our systems to prevent emails to that address. That enables us to prevent future contact using that email address. We do however always fully delete records on explicit request, although that does prevent us from including them in future exclude lists provided to partners and suppliers.

Your rights

It's your personal data and you have certain rights relating to it. When it comes to marketing communications, you can ask us not to send you these at any time – just follow the unsubscribe instructions contained in the marketing communication, or send your request to privacy@MD2MD.co.uk.

You also have rights to know what personal data we hold about you, and to make sure it's correct and up to date, to request a copy of your personal data, or ask us to restrict processing your personal data or and to have deleted information that we do not have to hold for legal or operational compliance reasons. You can exercise these rights at any time by sending an email to privacy@MD2MD.co.uk.

If you're not happy with how we are processing your personal data, please let us know by sending an email to privacy@MD2MD.co.uk. We will review and investigate your complaint, and try to get back to you within a reasonable time frame. You can also complain to your local data protection authority. They will be able to advise you how to submit a complaint.

Our policy is to make it as easy as possible for individuals to access their rights. In addition to automated processes, individuals can simply email privacy@MD2MD.co.uk with the request in clear normal English and an individual within our organisation will action the request as appropriate and confirm that has been done within a reasonable time. No fee is payable for any element.

We publish this policy and make links to it readily available so that individuals know this process.