GDPR STRATEGY & POLICIES

Gems Hygiene (Debonair (Northern) Limited)

Data Protection Officer, Gems Hygiene
chris@ghdirect.co.uk

Contents

Version Control

Version	Description of update	Date	Initial
V0.1	Draft version of GDPR policy – requires review	16/May/2018	JH

Our commitment to GDPR

Gems Hygiene provides cleaning products to schools, hospital, care homes and businesses within the UK. We use a frontline telemarketing team for inbound and outbound sales and account management based at a single site within Sheffield, UK.

We have produced this GDPR strategy to document our approaches to data privacy as we acknowledge that the laws surrounding data privacy and protection are changing. This includes being clear about how we process data, our purpose for processing personal data, recording our lawful basis for this, and identifying technological and operational measures that we must make to ensure data remains private and protected through a risk management strategy that considers **Data Privacy by Design**.

Data protection for building trust and integrity with our customers and our staff is central in providing our services. We aim to maintain and, whenever possible improve, on the minimum standards for the assurance of individuals' rights to data privacy and protection.

Dave Campbell, Managing Director, Gems Hygiene

Signed

Dated

Our GDPR Strategy

Our GDPR strategy aims to deliver operational and technological measures to protect the privacy of individuals whose data we process in order to deliver our automotive insurance and guarantee services.

This document presents the strategy in three sections.

Section 1 Understanding our data processes through audit of our operational and technological methods.

Section 2 Implementing procedures to communicate privacy information and to manage how we respond to access requests.

Section 3 Working with third parties to define responsibilities and ensure we can mutually protect data subjects' personal data.

GDPR is an ongoing process. This document will be reviewed annually and where appropriate, improvements will be made to maintain the privacy of personal data that we process.

1 Auditing Data Processing

We have undertaken a four point audit of our organisation in processing personal data.

1. An operational audit of our data processing activities (Section 1.1)
2. A technology audit of our data systems (Section 1.2)
3. Staff process audit and assignment of roles and responsibilities (Section 1.3)
4. Processes for responding to data breaches (Section 1.4)

In parallel to this we continuously manage risks to data privacy. We are able to identify, plan and implement appropriate measures to mitigate risk. This aligns with the GDPR requirement of 'Data Protection by Design'.

1.1 Operational audit

This section provides an audit of the relationship between our organisation, its systems for data processing and relationship with third parties (Figure 1).

Details of the data processes (P) and systems (S) are presented in Table 1.

An assessment of the risks and associated actions to take are logged in the corresponding document ***"Risk Log – Data Privacy & Protection"***.

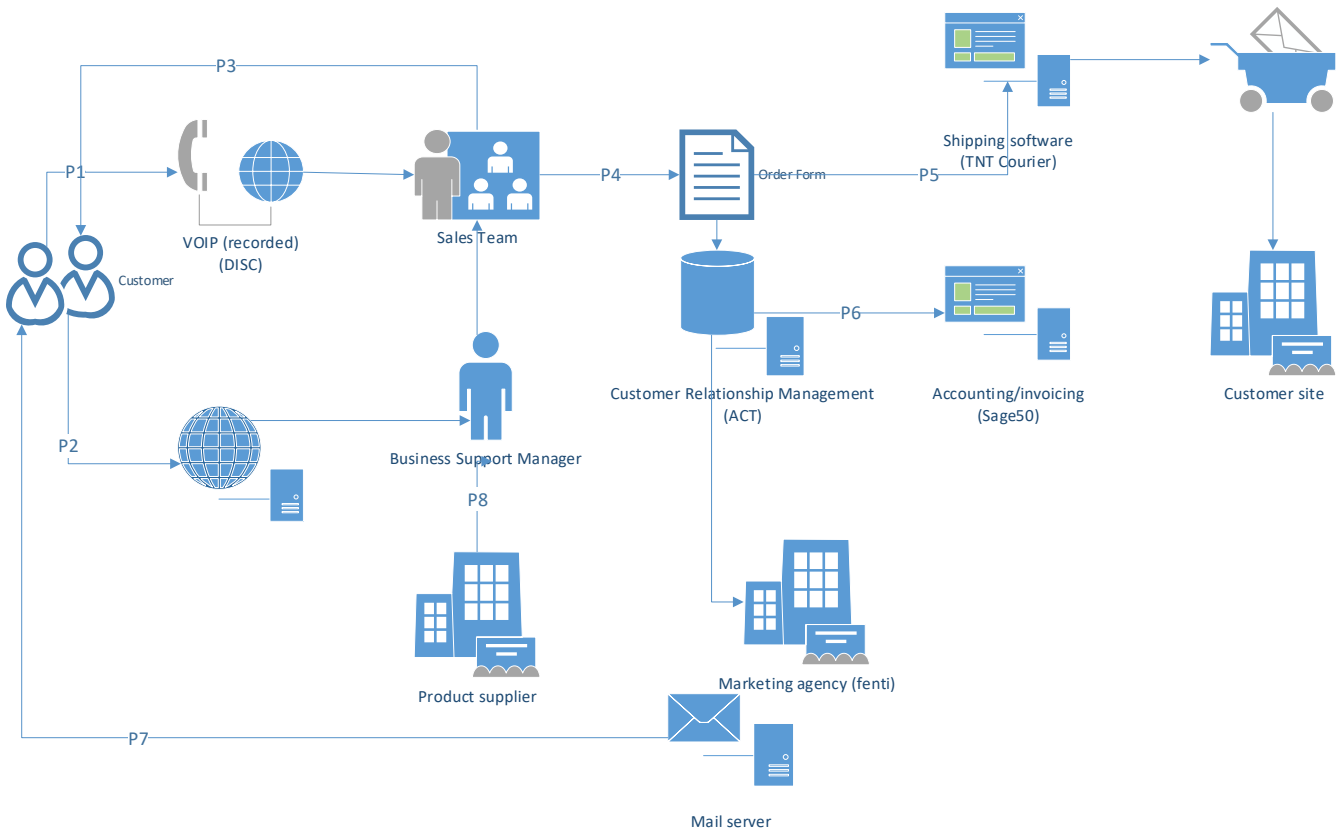

Figure 1 Gems Hygiene operations information systems audit map

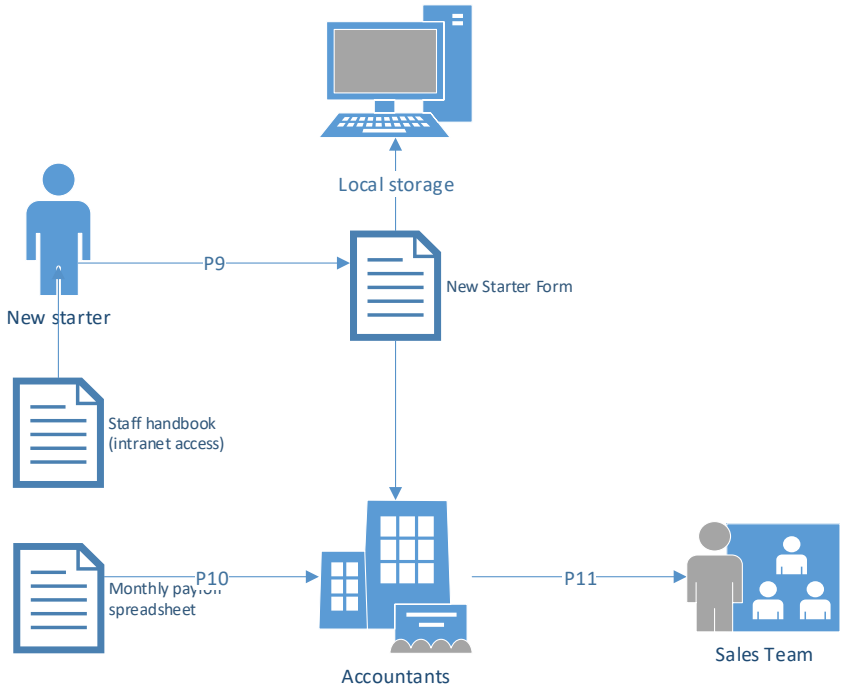

Figure 2 Gems Hygiene human resources information audit map

Table 1 lists the personal data we collect and process in order to provide our services.

System	Process (P)	Purpose limitation	Personal Data	Third Party Data Processor	Lawful basis	Retention Period	Privacy Statement (Y/N)?
Sales	P1	Inbound product enquiry, request for quote, orders	Name, address, email, phone number	No	Legitimate interest	Indefinite until moved in to 'feedback'.	Y
	P2	Inbound website enquiry	Name, email, telephone number	No	Legitimate interest	Indefinite	Y
	P3	Outbound telesales – new and existing customers	Name, telephone number	No	Legitimate interest	Indefinite	Y
Order processing	P4	Raising orders, purchase and shipping details	Name, address, email, phone number	No	Contract	6 years	Y
	P5	Shipping information & customer delivery	Name, address, delivery note details	Yes, TNT Courier	Contract	6 years	Y
	P6	Invoicing	Name, address	No	Contract	6 years	Y
Marketing	P7	Marketing campaign	name, email, company	Yes, fenti	Legitimate interest	Indefinite	Y
Supplier	P8	Product sourcing	Name, email, phone number, role	No	Legitimate interest	Indefinite	Y
Human resources	P9	Employee onboarding	Name, address, phone number, next of kin, medical info, emergency contact info, national insurance, passport (copy), attachment of earnings	Yes, accountants	Contract	Prospective employees – e.g. 6 months Current employees – e.g. 6 months after	Y

						employment ceased.	
	P10	Payroll (monthly)	Name, pay rate, commissions, pension, changes to address/contacts	Yes, accountants	Contract	6 years	Y
	P11	Postage of wage slips	Name, address	Yes, accountants	Contract	6 years	Y

Table 1 Gems Hygiene, Data Audit (use for audit and referencing with privacy statements)

1.2 Technology audit

Data privacy by design is adopted as part of our specification and requirements for selecting technology systems used for data processing. The specification steps include:

- Identify the purpose for which the system is intended
- Is the data processing necessary for the purpose (See Section 1.1)
- Can data items be removed and still achieve the intended purpose (‘***data minimisation’***?)
- Where does the data processing take place (‘***international transfer’?***)
- Is the technology supplier GDPR compliant (what assurances can they demonstrate to us?)

Each system is identified in Table 2.

System	Function	Offsite processing?	Is in EU?	Supplier	GDPR compliance?
Sales	Customer enquiries by phone	Yes	Yes	DISC	Yes
	Customer relationship management	No	Yes	ACT	Yes
	Invoicing customers	No	Yes	Sage50	Yes, see link
Marketing	Email marketing to new and existing customers	Yes	Yes	fenti ltd	Yes
Payroll	Paying employee wages	Yes	Yes	Accountants	Yes

Table 2 Gems Hygiene’s data processor compliance

Commented [JH1]: Are systems processing in EU zone?

Commented [JH2]: Contact suppliers for statement on GDPR

1.3 Staff audit

We train our staff to understand their responsibilities in helping Gems Hygiene maintain GDPR compliance. We specifically focus on the following areas:

- Notifying end users of their Rights through Privacy Statements
- Handling end users’ requests for data amendments and removals (our feedback process)
- Working with Data Processors (our Insurance and Finance partners)
- What to do in the event of a personal data breach.

We review annually our staff awareness of data privacy and protection. Our staff are trained in managing customer feedback relating to data accuracy. We have a CRM indexing system that allows staff to identify records that should be actioned (corrected, removed, restricted processing). Staff are also trained in their role and responsibility regarding data breach, what to do in the event of a data breach and highlight any risks that they see in day to day handling of personal data.

Roles

- Chris Hague (Business Support Manager, Gems Hygiene) is the appointed Data Manager
- Paul Campbell (Sales Manager) is the appointed Sales GDPR Trainer
- Jade Campbell (PA to MD) is the appointed Admin GDPR Trainer

1.4 Data breach handling audit

A personal data breach is the hack, destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to personal data. The impact to Gems Hygiene's Data Subjects is not severe, where there would be no impact to their individual rights. Nevertheless, we understand the impact that any data breach could cause to an individual's personal situation. All personal data breaches are recorded which forms part of our "***Data Privacy & Protection Risk & Incident log***". Our Data Manager will make a decision whether to inform the individuals affected based on assessment of the nature of the data breach and likely impact on data subjects.

.

2 Data Subjects' Rights

As a Data Controller we recognise our responsibility in responding to individuals' Rights. We manage this process by executing procedures in line with GDPR requirements for Data Subject Access Requests and prevention of data breaches in discharging our obligations during this process.

We coordinate Data Subject Access Requests through our Data Protection Officer, who is contacted by:

- Post: Data Manager, Gems Hygiene, 251 Sharrowvale Road, Sheffield, S11 8ZE
- Email: info@ghdirect.co.uk
- Phone: 0114 261 8187
- ***Data Protection Act 2018***

2.1 The right to be informed (privacy statements)

We will inform individuals of their right to object "at the point of first communication" and clearly lay this out in the following privacy notice. We have developed the following privacy statement which is embedded in documentation (either print or electronic) where we collate personal data.

GDPR and Data Protection Act 2018
Gems Hygiene Privacy Statement (Sales and order processing, online brochure, delivery notes, invoices, terms and conditions)

We are the **Data Controller** for the data **You** provide to **Us**. **We** use **Your** data for the purpose of contacting you or answering enquiries regarding product availability, to provide quotes, to fulfil your product order, shipping, and taking payment or issuing invoices.

We require your name, postal address, email, and phone number to fulfil your requirements for a quote or to receive goods. Our lawful basis for processing you data is **legitimate interest**.

We process all data in the UK but where **We** need to disclose data to parties outside the European Economic Area (EEA) **We** will take reasonable steps to ensure the privacy of **Your** data. **We** will retain **Your** data for as long as your remain a customer of Gems Hygiene. **We** have a Data Protection regime in place to oversee the effective and secure processing of **Your** data. Under GDPR legislation, **You** can ask **Us** for a copy of the data **We** hold, object to it being processed, have it corrected, sent to a third party or deleted. **We** will not make **Your** personal details available to any companies to use for their own marketing purposes. **You** must request a Data Subject Access Request Form from us to exercise Your Rights through us. **We** will respond within 30 days of receipt of your request. **You** must contact us by either writing, emailing or phoning the Data Manager, Gems Hygiene, 251 Sharrowvale Road, Sheffield S11 8ZE, info@ghdirect.co.uk, 0114 261 8187

If **You** wish to complain about how **We** have handled **Your** data, **You** can contact **Us** and **We** will investigate the matter. If **You** are not satisfied with **Our** response or believe **We** are processing **Your** data incorrectly **You** can complain to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF Tel: 0303 123 1113.

GDPR and Data Protection Act 2018
Gem's Hygiene Privacy Statement (Email Marketing)

OUR COMMITMENT to YOUR PRIVACY
You may have heard that there are some changes in data protection law that come in to effect this year. GDPR is giving you more control over how your data is used and how you wish to be contacted.

Our lawful basis for processing your information is legitimate interest. We have updated our Privacy Policy to reflect these changes. If you would like to find out more about what we are doing to protect your data, take a look at our Privacy Policy on our website.

You may opt-out from us contacting you. Or, you may ask us about our Data Privacy Policy by contacting our Data Manager by email: info@ghdirect.co.uk or by phone: 0114 261 8187 or by post: Data Manager, Gems Hygiene, 251 Sharrowvale Road, Sheffield, S11 8ZE.

GDPR and Data Protection Act 2018
Gems Hygiene Telephone Recorded Message

"We have updated our Privacy Policy to reflect changes in Data Privacy Laws. If you would like to find out more about what we are doing to protect your data, you will find our full Privacy Policy on our website."

GDPR and Data Protection Act 2018
Gems Hygiene Privacy Statement (for supplier contracts, agreements)

We are the **Data Controller** for the data **You** provide to **Us**. **We** need to use **Your** data so that we can make contact with your organisation for the purpose of procuring products under wholesale arrangements with **You**.

We require your name, postal address, email, and phone number to fulfil our ordering process. **Our** lawful basis for this is **legitimate interest**.

We process all data in the UK but where **We** need to disclose data to parties outside the European Economic Area (EEA) **We** will take reasonable steps to ensure the privacy of **Your** data. **We** will retain **Your** data for as long as your remain a supplier of Gems Hygiene. **We** have a Data Protection regime in place to oversee the effective and secure processing of **Your** data. Under GDPR legislation, **You** can ask **Us** for a copy of the data **We** hold, have it corrected, sent to a third party or deleted (subject to **Our** need to hold data for legal reasons). **We** will not make **Your** personal details available to any companies to use for their own marketing purposes. **You** must request a Data Subject Access Request Form from us to exercise Your Rights through us. **We** will respond within 30 days of receipt of your request. **You** must contact us by either writing, emailing or phoning the Data Manager, Gems Hygiene, 251 Sharrowvale Road, Sheffield S11 8ZE, info@ghdirect.co.uk, 0114 261 8187

If **You** wish to complain about how **We** have handled **Your** data, **You** can contact **Us** and **We** will investigate the matter. If **You** are not satisfied with **Our** response or believe **We** are processing

Your data incorrectly **You** can complain to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF Tel: 0303 123 1113.

GDPR and Data Protection Act 2018
Gems Hygiene Privacy Statement (Employee handbooks)

We hold a certain amount of data to support **Your** employment with **Us** including **Your** name, address, national insurance number, bank details, date of birth, next of kin, identification (passport, driving licence, other, including for use for evidence of right to work in UK), phone number, and any supplementary data that we are legally obliged to process, e.g. (any attachment of earnings.)

In addition **We** store **Your** CV, original application form/new starter list and any other documents which are relevant to **Your** employment – this may include details of disciplinary meetings or informal warnings, grievances, letters or references. **We** do not hold data for longer than it is necessary (6 months following cessation of **Your** employment.)

We process **Your** data in order to fulfil **Your** employment contract with **Us**. Contract is our lawful basis for processing under GDPR.

Following **Your** successful application of employment with **Us**, **We** may process medical data or family situational data (including maternity/paternity/child adoption arrangements, compassionate leave) to enable us to make special arrangements or reasonable adjustments within the workplace. In these special category cases, **We** will require **Your** consent for processing.

We share **Your** data with third parties in order to fulfil **Our** duties as **Your** employer which may include **Our** accountants, payroll, professional advisors, professional bodies or other organisations.

We process all data in the UK but where **We** need to disclose data to parties outside the European Economic Area (EEA) **We** will take reasonable steps to ensure the privacy of **Your** data. **We** will retain **Your** data for as long as your remain a supplier of Gems Hygiene. **We** have a Data Protection regime in place to oversee the effective and secure processing of **Your** data. Under GDPR legislation, **You** can ask **Us** for a copy of the data **We** hold, have it corrected, sent to a third party or deleted (subject to **Our** need to hold data for legal reasons). **We** will not make **Your** personal details available to any companies to use for their own marketing purposes. **You** must request a Data Subject Access Request Form from us to exercise Your Rights through us. **We** will respond within 30 days of receipt of your request. **You** must contact us by either writing, emailing or phoning the Data Manager, Gems Hygiene, 251 Sharrowvale Road, Sheffield S11 8ZE, info@ghdirect.co.uk, 0114 261 8187

If **You** wish to complain about how **We** have handled **Your** data, **You** can contact **Us** and **We** will investigate the matter. If **You** are not satisfied with **Our** response or believe **We** are processing **Your** data incorrectly **You** can complain to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF Tel: 0303 123 1113.

2.2 The right to object

You have the right to object to any processing undertaken for the purposes of direct marketing (including profiling). **We** will stop processing for direct marketing as soon as we receive your objection.

We will stop processing from the date of receipt of your objection.

2.3 The right to access

Should you wish to receive a record of the personal data that we hold about you, then we require you to contact us.

We will ask **you** to contact the Data Manager at Gems Hygiene (Data Manager, Gems Hygiene, 251 Sharrowvale Road, Sheffield S11 8ZE, info@ghdirect.co.uk, 0114 261 8187). **We** will respond within 40 calendar days of receipt of this DSAR. **We** also reserve the right to increase the response time to three months if we consider the request to be complex and time consuming. **You** have the right to contact the Information Commissioner's Office (ICO) if **you** disagree with **our** findings.

2.4 The right to rectification

We have implemented processes that ensure your personal data remains accurate and up to date. In the event data is deemed not accurate and you wish this data to be amended, **you** must contact us. You must specify which records you wish to be updated.

2.5 The right to erasure

At any time **you** may request that your personal data is erased from **our** records. **We** will erase all records in accordance with our storage and retention policy. **You** must provide details of the record **you** wish to be erased.

2.6 The right to restrict processing

You have the right to block or restrict the processing of your personal data. This means that **we** will store **your** personal data, but will not process it for further use in our marketing services. **We** will restrict processing under the following circumstances:

Where **you** contest the accuracy of the personal data, **we** will restrict processing until **we** have verified the accuracy of the personal data with **you**.

Where **you** object to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests) **we** will consider whether our businesses lawful basis override those of **you** as the individual. **We** will store the data, but will not undertake any further processing until both parties have agreed that our business use is within our lawful basis.

When processing is unlawful and the individual opposes erasure and requests restriction instead. **We** will store the data and will not undertake further processing. **We** refer you to the right to erasure policy, and will implement our erasure policy upon receiving your request.

Where **we** no longer need the personal data but you require the data to be retained to establish, exercise or defend a legal claim. **You** must state details of the record you wish to be retained. **We** will automatically delete personal data records in accordance with the consent policy. However, should **you** wish this data to be retained in order to establish, exercise or defend a legal claim, then **we** will store and retain this data until the legal claim has been resolved. **We** will inform you when **we** decide to lift a restriction on processing.

2.7 The right to data portability*

You have the right to obtain and reuse your personal data for your own purpose. **We** will provide **you** with your personal data or move, copy or transfer that data to another business in a safe and secure way.

The right to data portability only applies:

* to personal data **you** have provided us;

* where the processing is based on **your** consent or for the performance of a contract.

We will provide this data to you or the business to which you require your personal data to be transferred, within one month of receiving instruction from **you**. However, if we decide that the data request is complex, then **we** will extend this time period for a further two months. Where this is the case, **we** will provide an explanation.

Should **you** wish your data to be sent to you or transferred to another business, then **you** must contact the Data Controller to obtain a copy of a **Data Subject Access Request** form.

We will provide the personal data in a structured, commonly used and machine readable format. Examples of appropriate formats include CSV and XML files.

Where **we** are unable to transfer the data to another business due to technicalities or restrictions, then **we** will send the personal data to **you** for **you** to complete the transfer.

This service will be provided free of charge.

2.8 The right not to be subject to automated decision-making including profiling.

We do not perform automated decision-making using **your** personal data to profile, nor do **we** supply the information **we** hold to third parties for use in analysis or prediction.

3 Relationships with third parties

Our relationship in terms of GDPR with third parties means that we act as both a Data Controller and as a Data Processor. This section identifies the roles that we assume in each of these third party relationships. Our third party relationships include:

1. Accountant
2. Product suppliers
3. Marketing agency (emarketing)
4. Website support services

We issue **Data Processing Agreements** to clarify the responsibilities in each of these relationships.

Note to Data Protection Officer
**In the future, standard contractual clauses may be provided by the European Commission or the ICO, and may form part of certification schemes. However at the moment no standard clauses have been drafted.*
You are liable for your processor's compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor that adheres to an approved code of conduct or certification scheme may help you to satisfy this requirement – though again, no such schemes are currently available.

Processors must only act on your documented instructions. They will however have some direct responsibilities under the GDPR and may be subject to sanctions if they don't comply.
***Source: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/data-controllers/**

3.1 Accountants

We outsource our payroll to our accountants. We remain the Data Controllers of our employee data and payroll. Our accountant processes the payroll data. In this relationship the Accountant is a Data Processor and our staff are Data Subjects.

Staff are presented with privacy statements for their personal data processed by us and shared with our accountants via HR Privacy Statements held on Gems Hygiene intranet along with employee handbooks.

3.2 Product suppliers

We source the products that we sell from third party manufacturers. We hold individuals' personal information with whom we correspond to request orders for product supplies. We do not expect our Suppliers to process any personal information on our behalf.

3.3 Marketing agency (email marketing)

We use a third party for performing emarketing campaigns on our behalf. In this relationship we are the Data Controller and the agency is the Data Processor. We provide the agency with a list of contacts from our customer relationship management (CRM) database. We have in place a mutually binding agreement (Data Processor Agreement) with our emarketing provider.

3.4 Website support services

We employ an external website developer and host service from Intraspective (Sheffield, UK). In this relationship we are a Data Controller and the website service provider is the Data Processor.

4 Document Library

Document Name	Internal/External	Purpose	Where/when used
GDPR Strategy & Policy	Internal	Central document outlining Gems Hygiene's full GDPR strategy	Version controlled and should be updated periodically
Risk Log – Data Privacy & Protection	Internal	Live document detailing risks identified from GDPR Strategy & Policy document. Log of any incidences where personal data have been breached.	Reviewed annually.
Privacy Statements	External	Statement of Gems Hygiene use of data, identifying the lawful basis, retention policy, how to exercise rights.	Used for each case where data are being requested from a data subject. E.g. when completing webforms, phoning for a quote.
Data Processing Agreement	External	Communicates who is the Data Controller and Data Processor, associated responsibilities and lines of communication.	Issued to each supplier/ contractor working on behalf of Gems Hygiene, e.g. Payroll.

<ENDS>