sympatico

DOCUMENT: Napier Accounting: General Data Regulation (GDPR) Compliance, Risk and Gaps Report Pack

PREPARED FOR: Derek Napier, Napier Accounting ("YOU")

PREPARED BY: Sorcha Lorimer, Sympatico Consulting ("ME")

DATE: 7th August 2018

Executive Summary

Napier Accounting have commissioned Sympatico Consulting to assist them with compliance with the General Data Protection Regulation (GDPR). Specifically, this includes expert data risk and regulatory consultancy, compliance documentation creation (plan, inventory), privacy risk assessment via desk based review, and validation of efforts and select documents to date.

From Sympatico's discovery and analysis work on Napier's data flows, operations, processing activities and governance, Sympatico have determined and set out a number of recommendations and actions for Napier to consider in this report. These findings and associated actions should be reviewed alongside the custom created Napier GDPR plan and data audit, which are also detailed within this report and can be used as standalone compliance documents, and as a baseline and plan for you to maintain and update going forward. Sympatico recommend that scenarios relating to 'medium' risks within the risk and gaps table below should be prioritised.

Approach

Sorcha Lorimer worked through a detailed qualitative discovery stage with Derek Napier to uncover and map information flows at Napier (see Appendix II) and specifically where Personal Data (PD) is handled within your business operations. The focus was to uncover any vulnerabilities or examples of poor practice which might expose the business to risk, seek strategies to help mitigate those, build compliance and uncover opportunities for business optimisation. As an Accountancy business, Napier handle financial information on clients' behalf and demonstrating good data governance, security and a robust approach to compliance (with Data Protection and Financial regulations) is important, given the nature of your work and the need for client trust.

Based on the depth discovery interview, Sympatico created Napier's organisational data map, PD inventory (also know as the audit or record of authority), as well as the stages of completion of the GDPR implementation plan. Sorcha Lorimer then analysed the plan and assessed the inventory for privacy risks and gaps in relation to GDPR compliance at Napier. The output of that work is given in more detail below. (*Note that under GDPR Article 30, businesses with fewer that 250 employees are advised to focus on maintaining the inventory for high risk processing activities in particular, and there is a redaction for ad hoc and occasional processing; however, it is good practice to maintain an information inventory on a regular basis.*)

Compliance Risks and Gaps Summary & Recommendations

Below are the high level risks, recommendations and actions for Napier's attention, from analysis of your GDPR baseline (plan and audit as foundational), inventory, suppliers and processing activity, preparations to date and general business operations:

Reference/scenario	Business area	Details, Recommendations & Actions	Risk
Napier use cloud software for financial tasks and activities on behalf of clients, and work with a range of SMB clients; see Appendix II for further details. Agreements with your cloud processors tend to be on a self serve basis (see review notes below) Client engagement letters have not updated in line with GDPR at Napier There are no policies and procedures in place at Napier	Supplier & cloud services management Client management Legal	Ensure all supplier and client contracts, agreements between processors and controllers, and terms of engagement are compliant. All processing agreements to be in place or signed where Personal Data (PD) is being transferred between the data controller-data processor (and sub processors) - data subject at Napier. It also importance to gain compliance and security assurance on any processors Napier use (see Appendix I for high level). **Actions & Recommendations:** • Client letters/terms of engagement have not been updated in line with GDPR. These should be reviewed, updated and communicated to clients in line with GDPR as you are processing your clients' personal data. You can review and amend these at Napier or seek assistance from Sympatico or from your accounting body (ACCA). Updates should cover GDPR changes, how data will be used, roles, data sharing provisions and a link to your privacy policy • In future, ensure liabilities and responsibilities are covered where processing is taking place, and that suppliers are able to assure on GDPR compliance and security. Undertake due diligence for new suppliers or cloud services • Seek Data Processing Agreements (DPAs) or addendum from clients where PD processing is required.	**Medium** Focus on protecting Napier from liability exposure and assure current and new clients on compliance. Protect core business. Address gaps in agreements with PD is being processed

Reference/scenario	Business area	Details, Recommendations & Actions	Risk
Information handling at Napier is relatively limited and light touch With regards IT, this has been set up by your brother as an IT expert. Napier use OneDrive, and you have back ups and security measures in place e.g Bitdefender	Data governance at Napier IT Security	Napier currently save emails and prospects' personal data onto your network, in OneDrive. Napier also use an excel spreadsheet as a control document for all clients, again in OneDrive. This is a relatively secure location (given the back up strategy you shared and use of strategic and secure cloud storage), which is positive given this is personal data and high risk data (tax information, bank account details etc.) and thus should be protected. However, the storage of prospect emails is unstructured in current form. Napier print very little and take a digital first approach, which will bode well for upcoming Making Tax Digital (MTD) changes. When it comes to financial client tasks, you use a number of cloud software service providers (see Appendix I) for processing and accounting functions; this is positive as you benefit from automation and real-time information. When any documentation is printed, it is handled securely and confidentially. An important part of GDPR is upholding the data subjects' rights (to be informed, of access, to rectification, to erasure, portability, to restrict processing), for example Subject Access Requests (SARs). The processes and policies should always reflect the size and nature of the organisation and be appropriate and relevant for you. **Actions & Recommendations:** • Recommend creating a prospect control sheet and optimising non client data so that it is centrally stored, accurate and emails containing personal data which are not needed are deleted (GDPR stipulates data accuracy and minimisation) • Information Security is not simply about IT Security; consider role based access and physical security and storage (e.g. lockable storage) to protect sensitive information at Napier • Consider your approach to policies and procedures at Napier as you grow; it is recommended this is looked at. With regards GDPR: Data Protection and Information Security are key policies • Sympatico will create your draft Privacy policy, which should be finalised and added to your website/made available via a link to clients and subjects and where any data collection will occur • Look at how Napier would uphold a data subject request e.g. from a client • Review number of cloud vendors used • It would be useful to have a Records and Retention schedule at Napier and to identify business critical data to ensure it's protected, backed up and access is role based (for compliance and for business continuity) • Consider cyber essentials (or other) certification to protect your assets, assure clients and demonstrate commitment to Information Security for existing and new clients (e.g. tenders). Foundations include: secure: storage & IT, networks and disposal; boundary firewalls; malware protection; access & patch management, and a back up approach. Gain assurance from your IT provider (your brother) on security technical measures (e.g. which Bitdefender package) and back up approach.	**Low** Optimise information approach for data governance, particularly for prospect data, particularly where personal data is involved Gain regular assurance from IT on back ups and security Review policies and procedures

Reference/scenario	Business area	Details, Recommendations & Actions	Risk
Anti Money laundering regulations require accountants to undertake personal identity checks (using name, photograph, address and DOB), review risk and verify via documentary evidence, and then to keep a record of that This is not happening consistently and methodically at Napier	Financial regulatory compliance Client due diligence	Financial regulation compliance is out of the scope of this review; however, it is recommended that all compliance is considered to protect your business. Additionally, ID checks involve personal data, so this must be handled securely and processed in line with the regulation (i.e. clearly explaining personal data use and ensuring relevant lawful basis/gaining consent upfront tones clients). • Ensure compliance; optimise approach for collecting and processing personal data • Systemise and where relevant automate approach to ID checking to ensure compliance is upheld • Ensure personal and sensitive data is protected while in your care, through use of the relevant technical and organisational measures.	**Medium** Review and optimise approach to client due diligence in line with regulations
Napier undertake payroll activities for one of your clients, Taskforce. This involves processing of employee personal data via email	Operations	Historically, Taskforce shared employee payroll details via spreadsheets and email with Napier. **Actions & Recommendations:** • Email is an insecure means of communication, so consider organisational and technical measures or alternatives when sharing ay personal data via email (e.g. employee DP training, checks, encryption, dropbox, password protection om files) • Ensure Data Processing Agreement (DPA) is in place for future processing of a client's employees is in place (in this scenario, the employees are the data subject).	**Low/Medium** Review use of email and tighten up on DPAs going forward
Napier use an associated book-keeper	HR	Napier is a small business; you use a book-keeper who is not employed but works on a freelance basis **Actions & Recommendations:** • Consider associate agreement, with relevant DP clauses • Look at role based access and basic security awareness e.g Barclays guidance	**Low/Medium** Protect business with relevant contracts and agreements

Napier's Personal Data (PD) Inventory

Your data inventory is your compliance baseline and tells you where all of your Personal Data (PD) is and established legal bases, the provenance, retention periods etc. It also informs your privacy policy and notices, which should refer to your own data processing. This audit allows Napier to uncover gaps, risks, create your privacy policy and help facilitate data subject requests. It is one of the core documentation requirements for compliance under Article 30 of the GDPR obligations, as set out by the Information Commissioner's Office (ICO) (although there is a redaction for smaller businesses when it comes to low risk processing as noted previously).

Below is Napier's audit, based on information provided to Sympatico during the discovery phase; it is recommended that this record is used as a dynamic document and kept up to date at Napier on a regular basis, with a focus on any special category or high risk processing:

Why	Who (personal data)	What (type)	What (source)	What (legal basis)	When (updated)	When (retention period)	Where
Clients	Client contacts,	Name, email, address, telephone, tax information, bank account details. Some client employee data for payroll	1st party 2nd party (employees)	Contract	As required	On termination of relationship and in line with HMRC	OneDrive
Prospects	Personal contacts, legacy and prospects	Name, email, notes	1st party	Legitimate interests (need to validate that via regular review of LIA)	As required. Every 6 months	Delete when legal basis can no longer be established	Outlook; OneDrive
Business tasks	Client data	Contact and financial	1st party	Contract	As required, real time	On termination of relationship and in line with HMRC	Xero, FreeAgent, Taxcalc, Brightpay,
HR	Associate contact data	Name, email, telephone, financial	1st party	Contract	As required	6 years HMRC	OneDrive, email

Napier's GDPR Implementation and Compliance Plan

Another critical document as part of your requirements for compliance is your GDPR implementation plan, which is set out below:

Step/task	Goal	Who	How	By when	What has been done so far?	What's urgent? What's next?
Identify roles and responsibilities for Data Protection, governance and Information Security as part of GDPR	Align key roles and responsibilities so that GDPR compliance and Data Protection is embedded, with tasks and responsibilities clear	Derek Napier as sponsor; Sorcha Lorimer advisor	Via this 'project'	August 2018	Sponsor and expert aligned	Review recommendations and formulate into action plan with timescales for Napier. Consider approach for ongoing compliance
Audit, categorise & map data; Identify high risk or special category (e.g. financial) as focus as SME	Create baseline for Napier and identify high risk processing; goal would be to maintain this on regular basis	Sorcha Lorimer; Derek Napier	Via this 'project'	Set regular review dates	Data inventory created; high risk processing identified	Consider organisational and technical measures and your client policies when high risk data being processed (e.g. via email), such as encryption and checks on accuracy of address etc. as this email be a source of potential breach
Supply chain review: contracts, liability Are client & associate contracts or letters of engagement 'GDPR ready' - ensure safeguards, DPAs Client contracts and future projects consider GDPR	All DPAs in place and contracts and client documentation (letters of engagement) updated in line with GDPR and Data Protection.	Derek Napier	Existing documentation review and amend for GDPR	Ongoing	Initiated via this project	Sign DPAs for any processors Ensure agreements in place where PD processing taking place or where Napier could be exposed to any liability (e.g. Taskforce where employee data is being processes and transferred).
Review capabilities: security; data governance. Organisational & technical measures	Napier to have an approach to data governance and security which is appropriate for the nature of their work, size and at a sufficient level to assure clients	Sorcha Lorimer; Derek Napier	This review to provide initial recommendations at high level. Napier may seek guidance from IT/Security (via Derek's brother)	August; ongoing	IT set up in place; review undertaken with recommendations	IT security/IS foundations check with IT provider (brother) Create records and retention schedule Review some aspects of data handling (e.g. via email) as per recommendations from this project

Step/task	Goal	Who	How	By when	What has been done so far?	What's urgent? What's next?
Identify gaps, risks and priorities. Create plan	To mitigate any risks which could impact business operations	Sorcha Lorimer; Derek Napier	Via this 'project'; Work through key steps	Napier to define	Assessment created via this project	Mitigate any highlighted risks; focus on medium findings
Develop policies & processes: Data Governance framework. DSAR Process, DP & IS policies	Napier to have a data governance framework which is appropriate for the nature of their work, size and at a sufficient level to assure clients	Derek Napier	Consider company approach to policies and processes alongside growth plans	Napier to define	Recommendations and gaps reviewed	Identify goal and plan
Update marketing & communication: touchpoints.	External focussed communications and marketing to be compliant on an ongoing basis	Derek Napier	Website review complete; review any new comms for compliance	Napier to define	Website reviewed	Add privacy policy to website Add cookie banner if any analytics used on website
Train & communicate on GDPR	Napier to understand GDPR	Team to understand key points and principles; focus on team members who process PD	Consider training plan	Napier to define	N/A	Derek to understand basic principles (ICO documentation is good point of reference).
Data Breach Incident response plan	Napier to risk assess data breach incident and have a plan in place which is appropriate for business size and nature	Derek Napier	Discuss breach scenarios and key elements of plan (roles etc.)	Napier to define	N/A	Initial scenario discussion
Embed in culture at; ongoing part of internal and external approach	Napier to have a culture which upholds tenants of data protection and privacy by design so that compliance becomes integrated to operations	Derek Napier	Bring principles and best practice to life	Ongoing	N/A	Get up to speed on understanding of key principles

Conclusions, SWOT and Next steps

Overall there are no high findings which relate to special categories of data, high risk or known major security vulnerabilities which relate to risky data, and Napier are deemed to have a business model which limits data processing and is inherently digital first, as part of steps made towards Making Tax Digital and digitising aspects of data management at the company. In addition, Napier have typically selected strategic cloud technology which has been designed with security and privacy in mind from the outset.

However, attention should now be paid to documentation: agreements, letters of engagement, policies and any contracts to ensure they are aligned to GDPR and Data Protection principles (along with other Financial regulations, such as the anti-money laundering regulations), to ensure Napier are protected from liability, as well as demonstrating proper process to clients. Finally, Napier should consider training and processes, so that Data Protection and security are front of mind, for example when handling emails and other sensitive information.

High level Strengths, Weaknesses, Opportunities and Threats (SWOT) for Napier

Napier have a **STRONG** business model based on a trusted client base, which has been set up with modern and robust technology choices, relatively limited data processing, and a simplified operational model and supply chain.

A lack of written agreements/contracts, up to date letters of agreements, and loose or absent Information Security, Data Protection and Compliance policies and procedures is an area of **WEAKNESS.**

There are **OPPORTUNITIES** to optimise and document processes to re-assure existing or new (potentially larger) clients by formalising key processes for customers seeking assurance from Napier as their trusted accountant. One example of this is your letters of engagement with clients, in reviewing these, there may be an opportunity to make optimisations to existing arrangements with associated communications.

Potential **THREATS** include liabilities where data processing agreements are absent, and threats of fines or liabilities for non compliance with Data Protection or other Financial regulation. In addition lax IT security practices poses all businesses a threat without sufficient risk management of IT and Information and foundational controls.

Next steps

- Address risks and recommendations highlighted in this report; focus on medium findings
- Review GDPR plan and update with timeline which works for business
- Add Napier's public facing privacy policy on website etc., and consider other policies
- Maintain data inventory on regular basis; focus on high risk updates
- Consider records and retention schedule and associated data protection and data rights' procedures and policies.

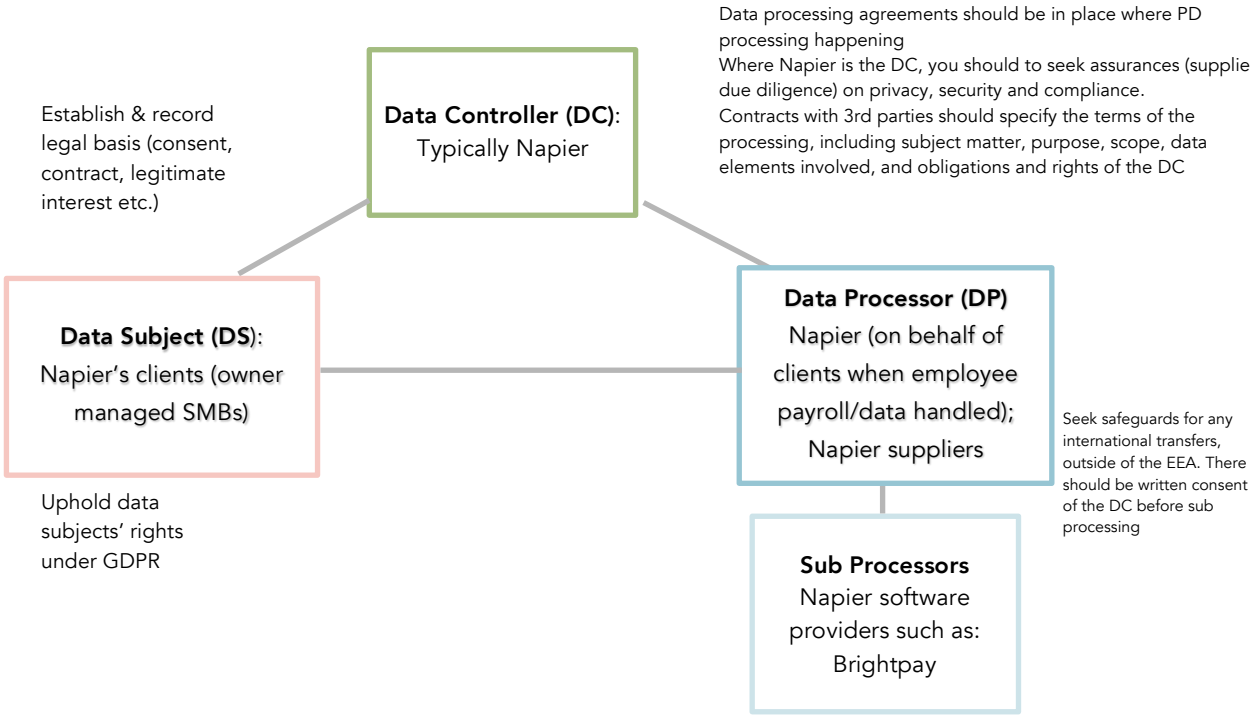
Appendix I

List of vendors used by Napier where (personal) data processing is involved.

Company	GDPR publicly available information	Observations, based on a desk based high-level review
Dropbox	Compliance journey	Dropbox have a solid reputation for security and taking compliance seriously, and it's part of their cole values. This comes over clearly in their publicly facing material
Xero	GDPR centre; DPA	Robust approach to GDPR & security. An NZ headquartered business, they use AWS servers in the US for hosting but ensure appropriate safeguards.
Brightpay	Brightpay and GDPR	Brightpay enables remote access to a secure and self service system for payroll; there are likely benefits for automated, accurate, backed up and secure payroll data in terms of supporting the principles of GDPR and good information governance. From reviewing their GDPR preparations information, the company also appear to take compliance and security seriously with a thorough approach. However, there are some aspects of their privacy policy and processing agreements which are unclear in terms of processing.
FreeAgent	GDPR preparations	FreeAgent look to have taken their and approach to compliance security seriously, and the implementation and approach approach looks robust, and from reviewing the privacy policy for users (there's a DPA for accountant partners, note), it is clarified that Freeagent use a number of sub processors located in EEA and US, such as Stripe, are used for processing users credit card details. Freeagent's servers are located in the UK. Freeagent appear to have a comprehensive understanding of security and compliance and have reviewed the adequacy of international transfers and sub-processing.
Taxcalc	Data Protection policies	From reviewing Taxcalc's publicly available privacy policies it's apparent they have undertaken GDPR compliance work, and that they take Information Security (IS) seriously with reference to relevant organisational and technical measures. They also have an appointed and named DPO. It should be noted that their data centres are in the UK; however, they do use third party sub processors.
Onedrive	Compliance centre	Microsoft take security and compliance seriously and have taken a rigorous approach and implemented relevant controls and industry recognised standards, as well as organisational and technical measures for good data management and robust IS. Note data location.

Appendix II

Napier's Organisational Information Map and Data flows at high level (which focusses on where personal data flows through your business); understanding your key data roles.



Sympatico's understanding of the Data Controllers, Data Processors, Sub Processors and Data Subjects in relation to Napier's business are as follows, at high level:

Data controllers
- Napier when handling client data
- Napier clients in relation to their employees

Data Processors & sub-processors:
- Napier when processing client data (e.g. payroll for employees as data subjects)
- Software and systems Napier uses when processing (personal) data, such as: Brightpay; FreeAgent; Xero; Dropbox, Taxcalc, Onedrive

Data subjects:
- Clients
- Employees or associates
- Prospects