PRAGMATIC

Third Party Service Providers

GSOC_Release_00.00.01_20180523

PRAGMATIC

Pragmatic Web Limited trading as 'Pragmatic' | 2nd Floor Chandos House, 26 North Street, Brighton, BN1 1EB | Company No. 07855805 | +44 1273 613166 | www.pragmatic.agency | ism@pragmatic.agency

Table of Contents

Introduction

GDPR requires Pragmatic to gain explicit consent from data subjects ahead of transferring their personal data to third countries (countries outside the EEA) or third parties (organisations that might gain access to that personal data).

We use numerous online third party service providers ("**service providers**") as integral parts of our business systems and operations. We simply cannot run our business without these services and, therefore, we must gain explicit consent from our clients (and all other data subjects) regarding the transfer of personal data to these service providers.

Rather than simply say that we might transfer your personal data to various organisations in multiple geographical locations (which many have taken as an expedient GDPR compliance solution in this context) we decided to conduct a data protection impact assessment on all our service providers (see below).

We include this list in our new GDPR compliant service contracts and, in so doing, provide clients (and other data subjects) with clear information regarding data protection provisions for each service provider we necessarily use.

How to Read The Table

Most of the columns in the table below are self explanatory.

The key columns for clients (and other data subjects) need to understand in order to asses the data protection credentials of each service provider we use are listed with notes below.

Geographically when outside the EEA

This column details where outside the EEA, if anywhere, each service provider stores the data we might transfer to them. If service providers store data outside of the EEA then they need to establish that their data protection practices meet the conditions laid down in Chapter 5 of GDPR. This column details how, if at all, each relevant service provider has met those conditions.

GDPR Chapter 5 Provision

What specific provisions has each service provider implemented to ensure that transfers of personal data outside of the EEA meet the conditions required by GDPR chapter 5.

DP Risk Assessment

This is our risk assessment of each service provider based on where the data is being stored, the GDPR chapter 5 provisions, the nature of the data being stored and how GDPR compliant each service provider is generally.

GDPR Compliant

A yes/no indication of GDPR compliance per service provider.

Third Party Service Provider Data Protection Impact Assessment

Operations & Communications

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Gsuite	CEO	Email, calendars, hangouts, documents etc	Extreme	Google Servers	USA, Taiwan, Singapore (more info)	EU Model Contract Clauses, Data Protection Amendment EU-US & Swiss-US Privacy Shields	Zero	✓	Like this and this	Restricted	High	High
Office365	CEO	Email, calendars, documents etc	High	Microsoft Servers	None (more info)	EU Model Contract Clauses EU-US & Swiss-US Privacy Shields	Zero	✓	Like this	Restricted	High	High

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Slack	ISM	Internal (and sometimes external) communications	High	Slack Servers	Unknown	International Data Transfers Privacy Shield And Contractual Terms EU-US & Swiss-US Privacy Shields Standard Contractual Clauses. See their GDPR statement for details.	Zero No data is transferred. Very limited personal data for access provisioned clients only.	✓	Like this	Internal	Low	High
Zoom	ISM	Video and web conferencing	Low	Zoom Servers	Unknown	EU-US & Swiss-US Privacy Shields Standard Contractual Clauses. See their privacy policy for details.	Zero Very limited personal data.	✓	Like this	Restricted	Medium	Low

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
AppearIn	ISM	Video collaboration/ conferencing	Low	AppearIn Servers	Unknown	None: See current privacy policy	Zero Very limited personal data.	✘	Like this	Restricted	Medium	Low
Join Me	ISM	Video conferencing	Low	Join Me Servers	n/a	EU-US & Swiss Privacy Shields	Zero No data is stored.	✓	Like this	Restricted	Medium	Low

Project Management, ticket tracking, task management & time logging

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Jira	ISM	Project management	Extreme	Atlas Host Servers	None.	Unnecessary. No transfers to third countries or international organisations.	Zero No data is transferred. Very limited personal data for access provisioned clients only.	✘	Like this	Restricted	High	High

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Trello	ISM	Project management	High	Trello servers	USA & Others unknown.	EU-US & Swiss-US Privacy Shields. See their privacy policy for details.	Zero Very limited personal data. Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	High
Workflow Max	ISM	Manages project workflows from quote through to invoice while tracking time and costs.	High	Workflow Max Servera	Unknown.	Adequate safeguards. See their privacy policy for details.	Zero Adequate safeguards.	✓	Like this	Restricted	High	High

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Basecamp	ISM	Project management	High	32Signals servers	Unknown.	EU-US & Swiss-US Privacy Shield policy	 Very limited personal data. Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	High
Freshdesk	ISM	Support ticket tracking	Extreme	Freshdesk servers	USA	EU-US & Swiss-EU Privacy Shields	 Very limited personal data. Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	High

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Smartsheets	ISM	Project plans, scheduled and timelines	Extreme	Smartsheet servers	USA & Others unknown.	EU-US & Swiss-US Privacy Shield. See their privacy policy for details.	 No personal data. Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	High
Usersnap	ISM	Client feedback and ticket tracking	High	Usersnap servers	None.	California Online Privacy Protection Act Compliance. See their privacy policy for details.	 Very limited personal data. Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	High

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Toggl	ISM	Time logging	Low	Toggl servers	Unknown.	Inadequate: See current privacy policy	 No personal data.	✘	See this	Restricted	Medium	Medium
Todoist	ISM	Task Management	Low	Todoist servers	USA.	Somewhat Inadequate: See current privacy policy & GDPR FAQ	 No personal data.	✘	Like this	Internal	Medium	Medium
Wunderlist	ISM	Task Management	Low	Microsoft Servers	None (more info)	EU Model Contract Clauses EU-US & Swiss-US Privacy Shields	 Secure infrastructure and privacy shielded.	✓	See this	Internal	Medium	Medium

Analytics & Diagnostics

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Ghost Inspector	ISM	Under The Bonnet customer website details	High	Ghost Inspector Servers	USA.	Adequate: See current privacy policy & GDPR Statement	 No personal data.	✓	Like this	Restricted	High	Medium

Documents & Documentation

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Confluence	ISM	Company Documentation	High	Atlas Host Servers	None.	Unnecessary? No transfers to third countries or international organisations?	Zero No data is transferred. Very limited personal data for access provisioned clients only.	✘	Like this	Restricted	High	High
GDrive	CEO	Internal documents of all kinds	Extreme	Google Servers	USA, Taiwan, Singapore (more info)	EU Model Contract Clauses, Data Protection Amendment EU-US & Swiss-US Privacy Shields	Zero Secure infrastructure and privacy shielded.	✓	Like this and this	Restricted	High	High

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Office365	CEO	Internal documents of all kinds	High	Microsoft Servers	None (more info)	EU Model Contract Clauses EU-US & Swiss-US Privacy Shields	 Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	High
Dropbox	ISM	Internal documents of all kinds	Extreme	Dropbox servers	USA.	Complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. See their privacy policy for details. EU-US & Swiss-US Privacy Shields	 Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	High

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Apple	ISM	iCloud for applications and document cloud management and storage	High	Apple servers	Unknown	EU Model Contract Clauses. See their privacy policy for details.	 Secure infrastructure and model contract clauses.	✓	Like this	Restricted	High	High
Evernote	ISM	Captures, organises, and shares notes within project teams.	Low	Evernote servers	Brasil, USA.	Standard Contractual Clauses. See their privacy policy for details.	 Very limited personal data. Privacy Shield Commitment.	✓	Like this	Internal	Medium	Medium

HR

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
BreatheHR	ISM	Employee records	High	BreatheHR Servers	None.	ICO Registration GDPR Statement of Compliance	Zero (for clients) because no clients data is stored here.	✓	Like this	Restricted	High	Low

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Office Vibe	ISM	Employee feedback information	Low	Office Vibe servers	Unknown.	Personal Information Protection and Electronic Documents Act ("PIPEDA"). See their privacy policy for details.	 (for clients) because no clients data is stored here.  Very low (for Pragmatic Staff)	✓	Like this	Restricted	High	Low

Sales, CRM & Marketing

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
HubSpot	ISM	CRM, Sales & Marketing, analytics and other contact information	Extreme	HubSpot Servers	Unknown.	Complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. See their privacy policy for details. EU-US & Swiss-US Privacy Shields	Zero Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	High
MailChimp	ISM	CRM, Email lists, customer communications and analytics	High	Mailchimp servers	USA.	EU-U.S. and Swiss-U.S. Privacy Shield	Zero Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	Medium

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
DotMailer	ISM	Email Marketing	Medium	Dotmailer servers	Unknown.	Standard Contractual Clauses. See their privacy policy for details.	 Limited personal data. Privacy Shield Commitment.	✓	Like this	Restricted	High	Medium
Eventbrite	ISM	Event publication, administration & attendee management	Medium	Eventbrite servers	USA.	EU-US Privacy Shield. See their privacy policy for details. EU-US & Swiss-US Privacy Shields	 Limited Personal Data. Secure infrastructure and privacy shielded.	✓	Like this	Restricted	Medium	Medium

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Chatlio	ISM	Sales support. Customer chat portal.	High	Chalio servers	Unknown	EU-US & Swiss-US Privacy Shields Coming Soon GDPR Compliance Statement	 Very limited personal data.	✓	?	Internal	Medium	Medium

Designer & Developer assets

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
WPEngine	ISM	Low level client website configurations and access portals	Extreme	WP Engine servers	None.	EU-US & Swiss-US Privacy Shields	Zero Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	Extreme
BitBucket	ISM	Code, DB & client asset repositories	Extreme	Bitbucket servers	USA	EU-US & Swiss-US Privacy Shields	Zero Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	High

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Github	ISM	Code, DB & client asset repositories	Extreme	Github servers	USA	EU-US & Swiss-US Privacy Shields	 Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	High
InVision	ISM	Full project design assets	Extreme	InVision servers	USA	EU-US & Swiss-EU Privacy Shields coming soon. See their privacy policy for details.	 Very limited personal data.	✓	Like this	Restricted	High	High
Zeplin	ISM	Full project design assets	High	Zeplin servers	USA	None.	 Very limited personal data.	✘	See this	Restricted	High	High

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Zapier	ISM	Customer website WordPress plugin hooks	Low	Zapier servers	USA	EU-U.S. Privacy Shield & U.S.-Swiss Safe Harbor Frameworks. See their privacy policy for details. EU-US & Swiss-US Privacy Shields	 Very limited personal data.	✓	Like this	Restricted	High	High

Finance

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Xero Accounting	ISM	Employee, customer and supplier data Accounting records	Extreme	Xero servers.	Unknown.	Adequate safeguards. See their privacy policy for details.	Low Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	High

Backup & Security

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Crashplan	ISM	Full backups of company computers. Anything and everything	Extreme	Crashplan servers	Unknown.	EU-U.S. Privacy Shield & U.S.-Swiss Safe Harbor Frameworks. See their privacy policy for details. EU-US & Swiss-US Privacy Shields	Low Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	High
Spanning Backup	ISM	Gsuite & Office365 Cloud to cloud backups	High	Spanning Backup servers	USA.	EU-U.S. Privacy Shield & U.S.-Swiss Safe Harbor Frameworks. See their privacy policy for details. EU-US & Swiss-US Privacy Shields	Low Secure infrastructure and privacy shielded.	✓	Like this	Restricted	High	High

Application	Asset Owner	Information Type	Criticality	Data Location & GDPR Compliance					Secured How	Security Classification		
				Physically held	Geographically when outside the EEA	GDPR Chapter 5 Provision	DP Risk Assessment	GDPR Compliant?		Confidentiality	Integrity	Availability
Sucuri	ISM	Customer website WordPress plugin hooks, virus data reports etc.	High	Sucuri servers	Unknown	None.	 No personal data.	No	n/a	Restricted	High	High
1-password	ISM	Passwords & potentially profiles (name, address etc), bank details (cards), notes	Extreme	1-password servers	USA	GDPR Compliance Statement	 No personal data.	✘	Like this	Restricted	High	Extreme
Sophos Anti-Virus	ISM	Malware scanning and removal	Extreme	No data held	Unknown.	Standard Contractual Clauses	 No personal data.	Yes	Like this	Restricted	High	High