

	Compliance Checklist	UK & EU	USA
US privacy laws at Federal and State level are creating a high privacy compliance hurdle for businesses trading with the US.	Awareness & Applicability		
	Identify laws which apply and how to comply (Federal laws (HIPAA (health); COPPA (children), ECPA (electronic communications), etc. States's laws.	GDPR PECR	Federal & State laws
	Training required by law?	✓	✓
	Data Mapping		
	Determine which data is affected	✓	✓
	Identify processing activities -	✓	✓
	Identify 'processors' or 'controllers'	✓	✓
	Identify 'legal bases'	✓	Consent
	Children & sensitive data - extra requirements	✓	✓
	Identify sources & recipients & location of data	✓	✓
EU and UK businesses can leverage their existing GDPR compliance framework to help overcome this hurdle.	Targeted advertising, profiling, 'cookies' – extra requirements	✓	✓
	Corporate Governance		
	Designate responsible personnel, implement 'accountability	✓	✓
	Data Protection Officer?	✓	✓
	EU (or UK) Representative?	✓	x
	Data Subjects' Rights		
	Must allow these rights to be exercised – implement systems	✓	✓
	Data subject access requests	✓	✓
	Documentation		
	Record Keeping: Log all decisions, assessments, incidents, DPIAs, LIAs, TIAs, TRAs, data flows (ROPA), breaches, notifications regarding breaches, Consents received for marketing, processing	✓	✓
Ash Costello advises on privacy law in the US and the UK, specialising in international transactions and cross-border privacy compliance and can address all your queries.	Data Privacy Impact Assessments template and register	✓	✓
	Data Processing Agreements (DPAs)	✓	✓
	Joint controller contract	✓	x
	Vendor due diligence (are they GDPR or US privacy law compliant?)	✓	✓
	Transparency & Communication		
	Website Privacy Policy/Notice disclosures	✓	✓
	Notices to data subjects about processing by third parties	✓	✓
	Employee notice, candidate notice, client notice	✓	✓
	Marketing notifications	✓	✓
	Consent management & notifications	✓	✓
	Breach notification to affected data subjects and regulators	✓	✓
	Cookie Notice	✓	✓
	Publish statistics on website - processing, breaches, DSARs	x	✓
	Notification about selling data	x	✓
	Policies and Procedures		
	Data processing policy - external	✓	✓
	Data processing policy – internal	✓	✓
	Policies on breach, retention, marketing, security, etc	✓	✓
	International data transfers		
	Restricted transfers, risk assessments, impact assessments	✓	Sensitive
	Security		
	Security mechanisms for data protection and cyber security.	✓	✓
	Breach management		
	Preparation, mitigation, responses	✓	✓

On Ash's website, she has compiled a list of *data regulator approved* compliance templates and checklists for you to download.

Contact Us | Ash Costello | Partner | Technology and Privacy | Licensed in NY & UK

www.gunnercooke.com | T: + 44 7555 923 203 | Telegram: @ashc0s | E: ash.costello@gunnercooke.com