For more information contact

Jon Dartley, Esq., 917-837-2909
jon@perlmanandperlman.com
www.perlmanandperlman.com

NEW YORK
41 Madison Avenue, Suite 4000
New York, New York 10010-2202
212|889.0575 phone
212|743.8120 fax

GDPR READINESS CHECKLIST

This GDPR Readiness Checklist sets out key requirements that the General Data Protection Regulation will introduce into EU Privacy law on 25 May 2018. The table highlights the most important actions that organizations should take to prepare for compliance, but please note that it is not a complete list of all actions/requirements, which will vary depending upon the organization and the nature of the information collected.

The changes enacted by the GDPR are wide-reaching and will require most organizations to make significant changes.. This checklist aims to identify, below, the stakeholders which will need to be involved in each set of actions.

- Legal
- Compliance
- HR
- IT & Information Services
- Insurance
- Security
- Procurement
- Marketing and Customer Relations
- PR & Communication

This table has been created with a B2C company in mind, i.e. a company obtaining, processing and storing quantities of consumer data. If an organization is B2B, while there may be certain areas where the obligations are slightly less onerous (and are less likely to require marketing and customer relations involvement), many of the requirements will still stand.

	Action(s) / Deliverables
Discovery/Governance	☐ Audit/Review all of the data you collect from users, and identify whether you are collecting information from individuals residing in the EU ☐ Document your Privacy Governance Model e.g. with clear roles and responsibilities and reporting lines to embed privacy compliance into the organization ☐ Consider whether a statutory DPO is required ☐ Review insurance coverage and consider whether it needs to be updated in light of the requirements of GDPR
Fair Processing and Consent	☐ Review your existing grounds for lawful processing and confirm that these will still be sufficient under the GDPR *e.g.* can you still rely on consent given the new requirements? ☐ Ensure that you are getting "explicit consent" in each instance; i.e. consent presented in a manner clearly distinguishable from other matters and in an intelligible and easily accessible form. ☐ Consider whether your organization is processing any sensitive personal data and ensure the requirements for processing such data are satisfied ☐ Where consent is relied upon as the ground for processing personal data, review existing consents to ensure they meet the GDPR requirements, and if not implement a process to seek new consents ☐ Ensure systems can accommodate withdrawal of consent
Children	☐ Identify whether you process personal data of children (under 16 for GDPR; 13 for US only) ☐ Seek local counsel advice regarding applicable local law restrictions, codes and guidance ☐ If data relating to a child will be processed, ensure that notices directed at that child are "child-friendly" and if consent is relied upon, you have implemented a mechanism to seek parental consent ☐ Consider alternative protections

Presented By: Jon Dartley, Esq., 917-837-2909
jon@perlmanandperlman.com or www.PerlmanandPerlman.com

Indvidual Rights and Procedures	☐ Update data privacy policy and internal processes for dealing with requests. ☐ Ensure technical and operational processes are in place to ensure data subjects' rights can be met, e.g. right to be forgotten, deletion of all data, data portability and the right to object
Record of Processing	☐ Identify all data processed in a detailed Record of Processing ☐ Implement and maintain processes for updating and maintaining Record of Processing
Privacy by Design and Default	☐ Ensure processes are in place to embed "privacy by design" into projects (*e.g.* technical and organizational measures are in place to ensure appropriate safeguards) ☐ Consider conducting a privacy impact assessment protocol
Compliant Contracting And **Procurement**	☐ Review all current contracts with vendors that collect GDPR-related data and implement a strategy for amending. ☐ Develop compliant contract wording for customer agreements and third-party vendor agreements ☐ Ensure procurement process has controls to ensure privacy by design (e.g. security diligence, data minimization, visibility of onwards data flows)
Data Breach Procedures	☐ Review and update (or develop where not in existence) Data Breach Response Plan ☐ Review insurance coverage for data breaches and consider whether it needs to be updated in light of the higher fines and penalties under the GDPR ☐ Review liability provisions in agreements for breaches caused by service providers and other partners

Presented By: Jon Dartley, Esq., 917-837-2909
jon@perlmanandperlman.com or www.PerlmanandPerlman.com