



# General Data Protection REGULATION

*Kegler Brown's Compliance Checklist*

**KEGLER  
BROWN  
HILL +  
RITTER**

**Our Privacy + Data Security team provides a practical approach for dealing with information security issues for global business operations**

<b>Governance</b>	GDPR introduces a number of requirements to ensure that compliance is a serious focus for companies.	5, 27, 37-39	<ul style="list-style-type: none"> <li>✓ Document Privacy Governance Model</li> <li>✓ Consider whether a statutory DPO is required</li> <li>✓ If no EU presence, appoint a local representative</li> <li>✓ Develop/administer employee training programs</li> </ul>
<b>Accountability</b>	Companies must document GDPR compliance programs.	5, 24, 25, 30	<ul style="list-style-type: none"> <li>✓ Implement a global overarching data protection policy</li> <li>✓ Integrate privacy compliance into your audit framework</li> </ul>
<b>Consent</b>	Data Subject must be able to withdraw consent from systems at any time.	5-10, 85- 91	<ul style="list-style-type: none"> <li>✓ Review existing consents to ensure they meet GDPR requirements</li> <li>✓ Ensure systems can accommodate withdrawal of consent</li> </ul>
<b>Notices</b>	Customers/employees must be adequately informed. Notice must be clear, concise, and informative.	10, 12-14	<ul style="list-style-type: none"> <li>✓ Review and update, where necessary, customer/employee notices to meet GDPR requirements</li> </ul>
<b>Data Subject Rights</b>	Ensure built-in right to access, right to be forgotten, and data portability.	16-23, 44-50	<ul style="list-style-type: none"> <li>✓ Update data privacy policy for dealing with requests</li> <li>✓ Ensure processes in place to satisfy data subjects' rights requests</li> </ul>
<b>Record of Processing</b>	Maintain a detailed record of all processing activities.	30	<ul style="list-style-type: none"> <li>✓ Identify all data processed in a detailed Record of Processing</li> <li>✓ Implement/maintain processes for updating Record of Processing</li> </ul>
<b>Privacy by Design</b>	Data protection plan must be designed at the outset, rather than later.	25, 35, 36	<ul style="list-style-type: none"> <li>✓ Embed privacy by design into projects</li> <li>✓ Put in place a privacy impact assessment protocol</li> </ul>
<b>Data Breach</b>	Must be provided within 72 hours of breach.	32-34	<ul style="list-style-type: none"> <li>✓ Review/update Data Breach Response Plan and insurance policies</li> </ul>



**Vinita Mehra**  
Director + Leader,  
Global Business Practice  
vmehra@keglerbrown.com  
614-255-5508



**David M. Wilson**  
Director + Co-Chair, Privacy +  
Data Security Practice  
dwilson@keglerbrown.com  
614-462-5406