The examination blueprint indicates the minimum and maximum number of items that are included on the CIPP/E examination from the major areas of the Body of Knowledge. Questions may be asked from any of the listed topics under each area. You can use this blueprint to guide your preparation for the CIPP/E examination.

**I. Introduction to European Data Protection**

<table>
<thead>
<tr>
<th>A. Origins and Historical Context of Data Protection Law</th>
<th>4 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rationale for data protection, human rights laws, early laws and regulations, the need for a harmonized European approach, the Treaty of Lisbon; a modernized framework</td>
<td>0 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B. European Union Institutions</th>
<th>42 69</th>
</tr>
</thead>
<tbody>
<tr>
<td>Council of Europe, European Court of Human Rights, European Parliament, European Commission, European Council, Court of Justice of the European Union</td>
<td>1 2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C. Legislative Framework</th>
<th>3 7</th>
</tr>
</thead>
</table>
E. Information Provision Obligations
   Transparency principle, privacy notices, layered notices

F. Data Subjects’ Rights
   Access, rectification, erasure and the right to be forgotten, restriction and objection, consent (and withdrawal of), automated decision making, including profiling, data portability, restrictions

G. Security of Personal Data
   Appropriate technical and organisational measures, breach notification, vendor management, data sharing

H. Accountability Requirements
   Responsibility of controllers and processors, data protection by design and by default, documentation and cooperation with regulators, data protection impact assessments (DPIAs), mandatory data protection officers, auditing of privacy programs

I. International Data Transfers
   Rationale for prohibition, adequate jurisdictions, Safe Harbor and Privacy Shield, Standard Contractual Clauses, Binding Corporate Rules (BCRs), codes of conduct and certifications, derogations, transfer impact assessments (TIAs)

J. Supervision and Enforcement
   Supervisory authorities and their powers, the European Data Protection Board, role of the European Data Protection Supervisor (EDPS)

K. Consequences for GDPR Violations
   Process and procedures, infringement and fines, data subject compensation

III. Compliance with European Data Protection Law and Regulation

A. Employment Relationships
   Legal basis for processing of employee data, storage of personnel records, workplace monitoring and data loss prevention, EU Works councils, whistleblowing systems, ‘Bring your own device’ (BYOD) programs

B. Surveillance Activities
   Surveillance by public authorities, interception of communications, closed-circuit television (CCTV), geolocation, biometrics/facial recognition

C. Direct Marketing
   Telemarketing, direct marketing, online behavioural targeting

D. Internet Technologies and Communications
   Cloud computing, web cookies, search engine marketing (SEM), social networking services, Artificial Intelligence (AI)