模拟题：概念和基本认知-GDPR（隐私保护）

1. 一家处理个人数据的公司正切换到另一家云提供商。切换之前必须检查哪些内容以确保GDPR合规？

A） 数据保护条例是否已变更

B） 数据保护控制是否合适

C） 处理者是否满足安全要求

D） 收集的数据是否仍足够且相关

答案：C

解释：

变更或引入下一级处理者要由控制者同意和审查，从控制者的角度来检查，看新处理者是否满足安全要求。

A和D是控制者的事。 B是具体技术方面的，不够全面。C包含B。

GDPR 第28条 第4款：

处理者引入其他处理者代表控制者进行特定处理活动的，第3 款项下控制者和处理者之间的合同或其他法律法规对数据保护义务应以欧盟或其成员国法律管辖的合同或其他法律法规的方式同样约束该其他处理者代表，特别是提供充分保证将采取适当的技术和组织措施以确保处理获得满足本条例要求。该其他处理者未能履行其数据保护义务的，最初处理者应就该其他处理者义务的履行对控制者承担全部责任。

1. 控制者必须在数据主体同意的情况下处理个人数据。没有任何其它合法的理由。处理过程中，控制者发现同意其进行处理的数据主体已死亡。

根据GDPR，控制者关于该处理后续会怎么做？

Ａ）控制者可按预期进行处理。

Ｂ）控制者可开始处理，但必须用于数据主体同意的目的。

Ｃ）控制者必须像数据主体已撤回同意一样行事，并删除其个人数据。

Ｄ）控制者要找到数据主体的继承人，以要求同意处理。

答案：A

GDPR对已故人士的数据不做规定。

对在世的人，遵循知情同意、合法必要、目的限制原则，目的限制其实是知情同意的延续；但对已故人士的数据，只需合法必要即可

1. 某人从Ａ市迁往B市。他是A市一家医院的病人。他现在要求医院将他的医疗档案直接转发到新的居住地B市的医院。

Ａ）Ａ市医院可将数据直接发给指定的Ｂ市的医院

Ｂ）Ａ市医院可以将医疗档案发送给数据主体，而不是发给另一家医院。

Ｃ）Ａ市医院无法遵守：敏感的个人数据只能在合法的基础上处理（发送）。

Ｄ）Ｂ市医院可以要求Ａ市的医疗档案，无需劳烦数据主体。

答案：A

解释：数据可携带权；

GDPR第20条：……技术可行的情况下，用户有权要求原始收集、存储其个人数据的企业直接将数据转移到另一企业。

1. 根据GDPR，监管机构应如何应对一个个人数据泄漏的通知？

A） 在处理数据泄露和采取减轻其后果的措施方面给控制者提供协助

B） 调查个人数据保护是否符合GDPR的安全要求。

C） 在由监管机构保存的数据处理公共登记册中记录数据泄露情况。

D） 如数据泄露可能对数据主体造成不利影响，向其报告数据泄露事件。

答案：C

解释：

A：监管机构提供咨询不提供协助。 监督机构还就处理作业提供咨询意见，或者是为了提高管制人员和处理人员对其在公布的公约下的义务的认识，或者针对控制者提出的协商要求或在发出数据泄露通知后进行调查的过程中提供咨询。

B是推行GDPR，进行监管的任务。不是泄露发生后的工作。

D是控制者要做的事。

监管机构这种情况下先记账，视影响以及控制者处理情况看要不要秋后算账

1. GDPR规定数据控制者需要与数据处理者签订书面合同（控制者不是处理者的情况下），以规范个人数据的保护。此类合同中内应包含某些具体条目。其中哪些条款是被期望包含的？

A） 说明保护个人数据所采取的具体技术措施的条款，以及授予控制者审查权的条款。

B） 要求处理者告知控制者数据是在哪个国家处理的条款，以及规定处理者需实施审计的条款。

C） 规定处理必须按照控制者的指示实施的条款，以及对处理者施加保密义务的条款。

D） 规定涉及任何下级处理者条件的条款，以及追究处理者不合规责任的条款。

答案：C

“按照控制者的指示实施”是处理者最主要的义务；

A不对，书面合同不要求具体技术细节。

B：所在国，GDPR中没有提到（好像中国比较在乎）； 处理者应协助控制者接受审计。（而不是实施审计。）

C：根据书面指示处理个人数据。处理数据的人员要承诺保密。

D：不需要具体涉及每一个下级（转包）处理者的条款，一般只需要做到这样就够：引入其他处理者时要经控制者同意，其他处理者同样受原合同约束，其他处理者不能履行义务的，原处理者要承担全部责任。

1. 发生了一起个人数据泄露事件，控制者正在起草一份通知给监管机构。这份文档中描述了泄露的性质及其后续的结果。其中还包含了能够给监管机构提供数据泄露额外信息的相关方信息。

控制者还应补充哪些其它信息？

A） 被通知的地方或国家机构的有关信息

B） 其数据遭泄露的数据主体的姓名和联系信息

C） 减轻数据泄露不良后果的措施的提议

D） 为查阅已被泄露的个人数据而所需的信息

答案：C

GDPR  第33 条 向监管机构通知个人数据泄露

通知至少应当包括：

(a) 对个人数据泄露的性质进行描述，包括涉及数据主体的类别和大致数量以及相关个人数据记录的种类和大致数量；

(b) 告知数据保护专员的姓名和联系方式，或者能获取更多信息的其他联络人；

(c) 描述个人信息泄露可能造成的后果；

(d) 描述控制者为弥补个人数据泄露采取的或计划采取的措施，包括降低潜在负面影响的措施。

A是指的被通知的监管机构，有个title就差不多了；B和D明显是进一步放大泄漏，肯定是不对的哈~~

1. 关于个人信息保护的“数据最小化”原则的含义是什么？

A） 个人资料应准确，必要时保持最新

B） 个人数据应对于处理目的足够即可，并限于处理目的的需要。

C） 个人数据的处理方式必须确保个人数据适当的安全性

D） 应以合法、公平且透明的方式处理与数据主体有关的个人数据

答案：B

解释：数据最小化是重要考点。

A是准确性

B正确，数据采集的最小化意指仅收集对于目的足够且必须的数据，数据用途的最小化即目的限制。

C是安全性

D是合法、公平、透明原则

1. 控制者可将个人数据处理外包给其他公司，前提是合作伙伴之间有签订书面协议。

该合同中的哪些条款是控制者的责任？

A） 确保授权处理个人数据的人员已承诺保密或承担适当的法定保密义务。

B） 提供证明遵守GDPR规定的义务所必需的所有信息，允许并促进包括检查在内的审计。

C） 仅根据书面指示处理个人数据，包括将个人数据传输到第三国或国际组织。

D） 以符合GDPR要求的处理方式，以适当的技术和组织措施提供充分保障。

答案：D

解释：

A、B、C是处理者的 见GDPR第28条，第3款）。

D见GDPR 第28条 第1款：

处理是以控制者的名义进行的，控制者只能使用那些能够充分保证在处理中采取恰当的技术和组织措施以满足本条例的要求、并且确保保护数据主体权利的处理者。

1. GDPR通常被称为欧洲隐私法。

数据保护和隐私之间有什么关系？

A）两者就是一回事（They are the same thing.）

Ｂ）数据保护是指保护个人隐私所需的措施（measures，很有可能被翻译成“度量”）

Ｃ）数据保护是隐私的一部分，其中涉及个人通信的保护。

Ｄ）数据保护是隐私的一部分，其中涉及个人数据的保护。

答案：Ｂ

解释：好像不用解释

1. 2016年7月12日，欧盟委员会实施了一项关于与美国转移个人数据的裁决(欧盟-美国隐私盾)。

对于GDPR来说，这是一个什么样的裁决？

A)充分性认定

B)例外法令

C)具有约束力的标准合同

D)取代GDPR的条约

答案：A

根据GDPR，欧盟委员会可以作出“充分性认定（an adequacy decision）”以承认一个国家或一个国家的一部分具备充分的数据保护（GDPR，第五章）。2016年7月，欧盟委员会颁布了2016 /1250号决议来承认**美国商务部**实施的欧盟-美国隐私盾计划所提供保护的充分性。