CIPP Exam Glossary

Find more at BareMetalCyber.com

1. **Accountability**
   Accountability is the requirement that an organization can *show* it complies, not just claim it complies. On the exam, it appears as questions about what evidence proves compliance (records, roles, policies, contracts), and it is often confused with general "good governance" that is not tied to demonstrable proof.

2. **Adequacy decision**
   An adequacy decision is a formal determination that a country or jurisdiction provides an essentially equivalent level of protection for personal data. On the exam, it commonly shows up in cross-border transfer scenarios where the "simplest lawful transfer path" is tested, and candidates often mix it up with contractual transfer tools.

3. **Anonymization**
   Anonymization is transforming data so an individual is no longer identifiable, meaning the result is not personal data under many privacy frameworks. On the exam, it matters because anonymized data changes which legal obligations apply, and it is frequently confused with pseudonymization, which still leaves data within scope.

4. **Automated decision-making**
   Automated decision-making is making decisions about individuals using automated processing, often including profiling, that can produce legal or similarly significant effects. On the exam, it appears as a rights-and-safeguards decision point, where you must identify when restrictions, transparency duties, or human review requirements are triggered.

5. **Binding Corporate Rules (BCRs)**
   Binding Corporate Rules are internal, approved rules that allow multinational groups to transfer personal data within the corporate group across borders under defined safeguards. On the exam, BCRs show up as a structured alternative to contract clauses, and the common trap is treating them like a quick template rather than a formally approved compliance mechanism.

6. **Consent**
   Consent is a specific legal permission that must meet quality conditions (for

example, being informed and freely given) and must be withdrawable. On the exam, the key is recognizing when consent is the right legal tool versus when another legal basis is more appropriate, and avoiding the mistake of treating notice as consent.

7. **Controller**
   A controller is the party that determines the purposes and means of processing personal data. On the exam, "who is the controller" often decides which obligations apply (notices, rights responses, governance), and it is commonly confused with a service provider that processes only on instructions.

8. **Data minimization**
   Data minimization means collecting and using only the personal data that is necessary for a specified purpose. On the exam, it shows up as "too much data for the stated purpose" scenarios, where the best answer is often to narrow collection, limit reuse, or shorten retention rather than add paperwork.

9. **Data processor**
   A processor is the party that processes personal data on behalf of the controller, typically under documented instructions. On the exam, processor status drives contract requirements, role separation, and accountability expectations, and a frequent confusion is assuming "vendor" automatically means "processor" without checking discretion and purpose.

10. **Data protection impact assessment (DPIA)**
    A DPIA is a structured risk assessment used when processing is likely to result in high risk to individuals, focusing on necessity, proportionality, risks, and mitigations. On the exam, DPIAs appear as "when is an assessment required" and "what must it cover" decision points, and the trap is treating it as optional paperwork instead of a required risk-control step in the right scenarios.

11. **Data Protection Officer (DPO)**
    A Data Protection Officer is an independent privacy role required in certain situations, responsible for advising on compliance and acting as a contact point for regulators and individuals. On the exam, this shows up as a "when is a DPO required and what can the DPO do" decision, and a common confusion is treating the DPO like a standard compliance manager who can be directed or penalized for doing the job.

12. **Data subject**
    A data subject is the identified or identifiable individual to whom personal data

relates. On the exam, data subject status drives which rights apply and how requests must be handled, and many questions test whether the person in the scenario is actually identifiable from the data described.

13. **Data transfer**
    A data transfer is a disclosure or movement of personal data to another party or location, especially across borders, that triggers specific safeguards under the applicable framework. On the exam, transfer questions test whether a cross-border mechanism is needed and whether the destination, recipient role, and onward sharing change the answer.

14. **De-identification**
    De-identification is reducing the link between data and a person, often by removing or altering direct identifiers, so identification becomes harder but not necessarily impossible. On the exam, it matters because de-identified data may still be regulated depending on re-identification risk, and it is often confused with true anonymization, which generally removes the data from scope.

15. **Derogation**
    A derogation is a limited exception that can permit certain processing or transfers when standard conditions are not met, usually under narrow, fact-specific rules. On the exam, derogations appear as “last resort” options, and the trap is selecting them as the default solution instead of using the primary lawful tools and safeguards.

16. **Direct marketing**
    Direct marketing is communicating promotional messages to individuals, often using personal data, and it can trigger specific rules on consent, opt-outs, and objections. On the exam, it shows up in scenarios about email campaigns, profiling for targeting, and the right to object, where the key is spotting the correct trigger and the required response.

17. **Encryption**
    Encryption is a security technique that transforms data into an unreadable form without the proper key, reducing exposure if data is intercepted or stolen. On the exam, encryption is tested as a safeguard and as a factor in incident and breach analysis, and candidates often over-assume it eliminates all legal duties regardless of key management and real risk.

18. **Erasure (right to)**
    Erasure is the right, in defined circumstances, for an individual to have personal

data deleted, often called the “right to be forgotten.” On the exam, it is tested through exceptions and conflicts (legal obligation, retention for claims, freedom of expression), where the best answer is frequently a documented partial refusal rather than automatic deletion.

19. **Establishment**
    Establishment refers to a real and effective presence of an organization in a jurisdiction, often connected to stable business activity. On the exam, establishment is a gateway concept for determining which law applies and which regulator is competent, and it is commonly confused with merely having customers or a website accessible in that region.

20. **European Data Protection Board (EDPB)**
    The European Data Protection Board is the EU body that promotes consistent application of data protection rules and issues guidance and dispute-resolution decisions in certain cases. On the exam, it appears in governance and enforcement context questions, where you must distinguish EDPB guidance and coordination from the powers of national supervisory authorities.

21. **Fairness**
    Fairness is the principle that personal data should be processed in ways people would reasonably expect and that do not cause unjustified harm or surprise. On the exam, fairness shows up as “lawful but still problematic” scenarios, where the best answer is often to change how processing is done or disclosed, not just to point to a legal basis.

22. **Filing system**
    A filing system is a structured set of personal data that is accessible according to specific criteria, including certain organized paper records. On the exam, this term appears in scope questions that test whether offline records fall under data protection rules, and it is commonly confused with any random paper stack that is not meaningfully organized.

23. **Freely given**
    Freely given means consent is not valid if it is coerced, bundled improperly, or tied to a service in a way that removes real choice. On the exam, it shows up in consent-quality questions, especially in employment or essential-service contexts, where the correct move is often to pick a different lawful basis.

24. **Further processing**
    Further processing is using personal data for a new purpose beyond the original reason it was collected. On the exam, it is tested as a compatibility decision: whether the new purpose fits the original context, what safeguards are needed, and when a new legal basis or notice is required.

25. **General Data Protection Regulation (GDPR)**
    The General Data Protection Regulation is the EU-wide legal framework governing personal data processing, including roles, rights, and enforcement. On the exam, it functions as the core reference model for concepts like controller versus processor, lawful bases, and transfer mechanisms, and many questions test whether you can apply those rules to a fact pattern rather than recite them.

26. **Joint controllers**
    Joint controllers are two or more parties that jointly determine the purposes and means of processing. On the exam, this matters because it changes accountability and transparency expectations, and the common confusion is assuming joint controller status just because two parties both touch the data, even if one party only follows instructions.

27. **Lawful basis**
    A lawful basis is the legally recognized ground that permits processing, such as consent, contract necessity, legal obligation, vital interests, public task, or legitimate interests. On the exam, choosing the correct lawful basis is a top decision point, and wrong answers often pick consent by default even when another basis fits better and reduces compliance risk.

28. **Legitimate interest**
    Legitimate interest is a lawful basis that can support processing when the organization's interest is not overridden by the individual's rights and freedoms, usually requiring a balancing analysis. On the exam, it appears in marketing, fraud prevention, analytics, and internal operations scenarios, and the trap is skipping the balancing logic and safeguards that make this basis defensible.

29. **Onward transfer**
    Onward transfer is a further transfer of personal data from the initial recipient to another recipient, often in another country. On the exam, this tests whether the original transfer safeguards still protect the data after it moves again, and

candidates often miss that the second transfer can create new compliance requirements.

30. **Personal data**
    Personal data is any information relating to an identified or identifiable person, including indirect identifiers when combined with other data. On the exam, this is a foundational scope concept that drives almost every scenario, and common mistakes involve treating device identifiers, location traces, or unique account activity as “not personal” when they can reasonably link back to a person.

31. **Personal data breach**
    A personal data breach is a security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. On the exam, this shows up as “is this a breach and what happens next” logic, where the key is the risk to individuals, not just whether a system alert fired.

32. **Privacy by design**
    Privacy by design means building privacy safeguards into systems and processes from the start, rather than bolting them on later. On the exam, it appears as questions about choosing default settings, limiting collection, and designing controls that support rights handling, and it is often confused with writing a policy after deployment.

33. **Privacy impact assessment (PIA)**
    A privacy impact assessment is a structured review of how a project affects privacy risks, what data is involved, and what mitigations are needed. On the exam, PIAs show up as the practical mechanism for demonstrating accountability and risk-based thinking, and the common trap is treating the assessment as optional documentation instead of a decision tool.

34. **Processing**
    Processing is any operation performed on personal data, such as collecting, storing, using, sharing, analyzing, or deleting. On the exam, the term matters because it defines the scope of obligations, and many questions test whether a seemingly simple activity like “viewing” or “logging” is still processing.

35. **Profiling**
    Profiling is automated processing used to evaluate personal aspects of a person, such as behavior, preferences, reliability, or location patterns. On the exam, profiling shows up in advertising, risk scoring, and fraud detection scenarios, and it

is commonly confused with basic segmentation that is not meaningfully predictive or impactful.

36. **Pseudonymization**
    Pseudonymization is replacing identifiers with a code or token so data is less directly linked to a person, while still allowing re-linking under controlled conditions. On the exam, it matters because pseudonymized data is still personal data, and a frequent mistake is treating it as anonymized and therefore out of scope.

37. **Purpose limitation**
    Purpose limitation means personal data should be collected for specific, explicit purposes and not reused in incompatible ways. On the exam, this appears when a scenario introduces a "new use" for existing data, and the decision hinges on compatibility, transparency, and whether a new legal basis is needed.

38. **Record of processing activities (ROPA)**
    A record of processing activities is a documented inventory of processing that captures what data is processed, why, by whom, for how long, and with what safeguards. On the exam, it shows up as evidence of accountability and governance, and candidates often confuse it with a data map even though it must support compliance decisions and auditability.

39. **Rectification (right to)**
    Rectification is the right for individuals to have inaccurate personal data corrected, and in some cases completed. On the exam, this is tested in rights-handling scenarios where accuracy affects outcomes, and the trap is treating rectification like deletion rather than a targeted correction with a documented response.

40. **Restriction of processing**
    Restriction of processing is limiting what can be done with personal data while keeping it stored, often as a temporary control during disputes, objections, or verification. On the exam, it appears as an alternative to deletion when a legal or factual issue is unresolved, and it is commonly mistaken for a full stop that eliminates all processing obligations.

41. **Sensitive data**
    Sensitive data is personal data that carries higher risk to individuals if misused, such as health details, biometric identifiers, or precise location, depending on the legal framework. On the exam, the presence of sensitive data usually changes the

required safeguards, the consent or lawful basis analysis, and the risk assessment expectations, so it is often the first “trigger” to spot.

42. **Special categories of personal data**
    Special categories of personal data are defined types of highly protected data under European frameworks, commonly including things like health data, biometric data used for identification, and data revealing political opinions or religious beliefs. On the exam, this term matters because it adds an extra layer of conditions for lawful processing, and many wrong answers treat it like normal personal data with only standard controls.

43. **Standard Contractual Clauses (SCCs)**
    Standard Contractual Clauses are approved contract terms used to add safeguards for certain international transfers of personal data. On the exam, SCCs show up as a common transfer mechanism selection, and the frequent confusion is thinking the clauses alone finish the job when the scenario suggests extra risk evaluation or supplementary measures may be needed.

44. **Storage limitation**
    Storage limitation means keeping personal data only as long as needed for the stated purpose, then deleting or truly anonymizing it. On the exam, this appears in retention and “just in case” storage scenarios, where the best answer is usually a defined retention schedule tied to purpose and legal requirements, not indefinite storage.

45. **Supervisory authority**
    A supervisory authority is the national regulator responsible for enforcing data protection law and handling complaints, investigations, and penalties. On the exam, this concept appears in enforcement and incident response questions, where you must know when regulator notice is required and how authority jurisdiction can depend on establishment and processing context.

46. **Third country**
    A third country is a country outside the relevant regulated area, such as outside the European Economic Area in European privacy contexts. On the exam, the term is used to signal that a cross-border transfer analysis is required, and candidates often miss that “remote access” or cloud processing can still involve a third-country transfer.

47. **Transparency**
    Transparency means people can understand what data is collected, why it is used, who receives it, and what rights they have, presented in a clear and accessible way. On the exam, transparency is tested through notice content and timing decisions, and a common trap is selecting a security control when the real gap is unclear or late disclosure.

48. **Transfer impact assessment (TIA)**
    A transfer impact assessment is a structured evaluation of risks associated with transferring personal data internationally, including whether the destination's laws and practices undermine the intended safeguards. On the exam, it appears as the "additional step" that turns a transfer tool into a defensible decision, and wrong answers often skip it when the fact pattern hints at elevated access or government risk.

49. **Unambiguous consent**
    Unambiguous consent is consent expressed through a clear affirmative action that leaves no reasonable doubt about the individual's agreement. On the exam, it is tested in interface and notice scenarios, where silence, pre-checked boxes, or vague acceptance language typically fails the standard and leads to the wrong legal basis choice.

50. **Vital interests**
    Vital interests is a lawful basis that can permit processing when it is necessary to protect someone's life or physical safety. On the exam, this term shows up in emergency scenarios, and the common confusion is using it to justify routine business processing when the facts do not meet the high threshold.