Given the following 3 exerpts :

30. "Therefore, you must assess, where appropriate in collaboration with the importer, if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the Article 46 GDPR transfer tool you are relying on, in the context of your specific transfer. Where appropriate, your data importer should provide you with the relevant sources and information relating to the third country in which it is established and the laws applicable to the transfer. You may also refer to other sources of information, such as the ones listed non-exhaustively in Annex 3."

99. "The exporter could add annexes to the contract with information that the importer would provide, based on its best efforts, on the access to data by public authorities, including in the field of intelligence provided the legislation complies with the EDPB European Essential Guarantees, in the destination country."

Footnote 49: "FISA 702 is applicable if the data is obtained “from or with the assistance of an electronic communication service provider” (Section 702 FISA = 50 USC § 1881a, under (h)(2)(A)(vi)), which in turn is defined in 50 USC § 1881(b)(4) as
“(A) a telecommunications carrier, as that term is defined in section 153 of title 47;
(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18;
(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18;
(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or
(E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).”

Wouldn't it be in the scope of the EDPD's mission, in the given context, to analyse a set of well-known US importers and simply inform us wether or not they are in the scope or not of the given FISA 702 law? That would be much more effective and less of a burden to the exporter.

==========
Use case 1 :

"the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them,"

is in pure contradiction with

42. "... you should look into other relevant and objective factors, and not rely on

subjective ones such as the likelihood of public authorities' access to your data in a manner not in line with EU standards."

Indeed, how one can NOT "objectively" assess the resources and technical capabilities of a public authority. It can only be a guess. No country ever publicies such cybersecurity/military capabilities.

Based on
- the permanent wire taping of network flows the NSA as describe in the CJUE ruling arguments numbers 62 and 63 ;
- and any related serious literature and study such as : https://arstechnica.com/information-technology/2015/10/how-the-nsa-can-break-trillions-of-encrypted-web-and-vpn-connections/ ;

any person applying simple but still "subjective" reasonning would conclude that US "resources and technical capabilities" will always "beat" any encryption standard in the long run. They are tapping the wire permanently, so as far as time and resources allows it, the data will end up being decrypted.

As a conclusion :
- It could sound not to set aside the "likelhood". Hence the "risk" based approach behind the GDPR.
- Concerning the public authorities capabilities, it might be fair to inform somewhere in the recommandation document about the constant wire tapping taking place, as the CJEU does, and give advice about using best practice sate-of-the-art data in transit encryption techniques (prime numbers selection randomness, prime numbers siyes, etc.).
- As for the data at rest, to align with the encryption recommandations of the public authorities of the importers made either to its governement bodies (US governemental bodies are required to use AES 256 bits or so, somewhere in their documentation...) or to its private sector (see FedRAMP security standards imposed to the private sector willing to provide something to the US governement agencies).

==========
Use case 5 :

"Similarly, public authorities of either country should not have the authority to access personal data held by processors in all jurisdictions concerned."

We know that as for the CLOUD Act, any subsidiaries of a US company will have to comply with a request of disclosure even the data is in the EU. Unfortunately, the CJEU does not make any mention of this act. Is there, here, an opportunity pin point that or to rephrase?

==========
Use case 6 :

This use case leaves too much room for interpretation. Indeed, it is specified that there should be a "need" to acces data in clear from the provider perspective. Any cloud processor stating in their terms and conditions that they do not "need" to

access the data would therefore be cleared from this use case. And from false correlation of the being not concerned with this use case and any other use cases, exporter and importer can falsely conclude that the cloud provider is compliant.

For example, AWS data processing addendum states that they do not "need" to access your data, unless... :

"AWS will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order)."

While Microsoft views the "need" to access data from quite wide perspective. No ownership, but a license to use it, which entails an inevitable access to it :

"We don’t claim ownership of Your Content. Your Content remains Your Content...you grant to Microsoft a worldwide and royalty-free intellectual property license to use Your Content, for example, to make copies of, retain, transmit, reformat, display, and distribute via communication tools Your Content on the Services."

As a conclusion, most cloud provider do not "need" to access data, unless required by law, or are granted to use it anyway, as stated in their respective terms.

==========
Use case 6 (second argument):

Microsoft which use personal data to identify person via Azure AD, can not technical ensure the encryption of such data at rest whith the importer not being in possession of encryption keys.

Microsoft "needs" to access to that data in order for the complete Azure platform to function.

Given this use case, controllers taking advantages of Microsoft and any other US service provider providing similar services (and pratically any type of service including identification/authentification personal data), would be doomed to suspend the transfer of data. Which pratically means disconnect most EU administrations and big companies from the Internet.

==========
About CLOUD Act

Microsoft participates to the PRISM surveillance program referenced in the CJUE ruling.

Microsoft Ireland which is a subsidiary to Microsoft Corporation, is the main contractor for EU controllers.

In addition to the FISA 702 and EO12333 mentionned in the CJUE ruling, Microsoft is also subject to CLOUD Act. It must comply with a court order, including its

subsidairies. Any data residing in EU territory must be handed over and given access to.

This act, even if not mentionned in the CJEU ruling applys.

FISA being mentionned in this recommandation, one may wonder why there is no use case specific to subsidiaries issue regarding such impinging laws, and to the Cloud act moe specifically.