Please see below my review of possible requirements contained within the Article 29-Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC

DC – Data Controller

[DC-D1-R1]

Article 7 requires that personal data shall only be processed if at least one of six legal grounds listed in that Article apply. In particular, personal data shall only be processed (a) based on the data subject's unambiguous consent; or if - briefly put - processing is necessary for:

(b) Performance of a contract with the data subject;

(c) Compliance with a legal obligation imposed on the controller;

(d) Protection of the vital interests of the data subject;

(e) Performance of a task carried out in the public interest; or

(f) Legitimate interests pursued by the controller, subject to an additional balancing test against the data subject’s rights and interests.

[DC-D1-R2]

The Work Programme itself clearly stated two objectives: 'ensuring the correct implementation of the current legal framework' and also 'preparing for the future'.

[DC-D1-R3]

Article 8 of the European Convention on Human Rights, adopted in 1950, incorporates the right to privacy - i.e. respect for everyone's private and family life, home and correspondence. It prohibits any interference with the right to privacy except if ‘in accordance with the law' and 'necessary in a democratic society' in order to satisfy certain types of specifically listed, compelling public interests.

[DC-D1-R4]

Article 8 ECHR focuses on the protection of private life, and requires justification for any interference with privacy. This approach is based on a general prohibition of interference with the right of privacy and allows exceptions only under strictly defined conditions. In cases where there is 'interference with privacy' a legal basis is required, as well as the specification of a legitimate purpose as a precondition to assess the necessity of the interference.

[DC-D1-R5]

The Charter enshrines the protection of personal data as a fundamental right under Article 8, which is distinct from the respect for private and family life under Article 7. Article 8 lays down the requirement for a legitimate basis for the processing. In particular, it provides that personal data must be processed 'on the basis of the consent of the person concerned or some other legitimate basis laid down by law'. These provisions reinforce both the importance of the principle of lawfulness and the need for an adequate legal basis for the processing of personal data.

[DC-D1-R6]

This Section III provides a brief overview of each of the legal grounds in Article 7(a) through (e) of the Directive, before the Opinion focuses, in Section III, on Article 7(f). This analysis will also highlight some of the most common interfaces between these legal grounds, for instance involving 'contract', 'legal obligation' and 'legitimate interest', depending upon the particular context and the facts of the case.

[DC-D1-R7]

It has an important role, but this does not exclude the possibility, depending on the context, that other legal grounds may be more appropriate either from the controller’s or from the data subject’s perspective. If it is correctly used, consent is a tool giving the data subject control over the processing of his data. If incorrectly used, the data subject’s control becomes illusory and consent constitutes an inappropriate basis for processing.

[DC-D1-R8]

"Clarification should aim at emphasizing that unambiguous consent requires the use of mechanisms that leave no doubt of the data subject’s intention to consent. At the same time it should be made clear that the use of default options which the data subject is required to modify in order to reject the processing (consent based on silence) does not in itself constitute unambiguous consent. This is especially true in the on-line environment." It also required data controllers to put in place mechanisms to demonstrate consent (within a general accountability obligation) and requested the legislator to add an explicit requirement regarding the quality and accessibility of the information forming the basis for consent.

[DC-D1-R9]

There is a clear connection here between the assessment of necessity and compliance with the purpose limitation principle. It is important to determine the exact *rationale* of the contract, i.e. its substance and fundamental objective, as it is against this that it will be tested whether the data processing is necessary for its performance. In some borderline situations it may be arguable, or may require more specific fact-finding to determine whether processing is necessary for the performance of the contract.

[DC-D1-R10]

Fraud prevention - which may include, among others, monitoring and profiling customers - is another typical area, which is likely to be considered as going beyond what is necessary for the performance of a contract. Such processing could then still be legitimate under another ground of Article 7, for instance, consent where appropriate, a legal obligation or the legitimate interest of the controller (Article 7(a), (c) or (f)). In the latter case, the processing should be subject to additional safeguards and measures to adequately protect the interests or rights and freedoms of data subjects.

Article 7(b) only applies to what is necessary for the *performance* of a contract. It does not apply to all further actions triggered by non-compliance or to all other incidents in the execution of a contract. As long as processing covers the normal execution of a contract, it could fall within Article 7(b).

[DC-D1-R11]

Article 7(d) provides for a legal ground in situations where ‘processing is necessary in order to protect the vital interests of the data subject’. This wording is different to the language used in Article 8(2)(c) which is more specific and refers to situations where ‘processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent’.

[DC-D1-R12]

Recital 27 of this Regulation 45/2001 provides that ‘processing of personal data for the performance of tasks carried out *in the public interest* by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies.’ This provision thus allows data processing on a broadly interpreted ‘public task’ ground in a large variety of cases, which could have otherwise been covered by a provision similar to Article 7(f).

From this point not sure how these may be considered as requirements but will included as my knowledge of data controller is not exact

[DC-D1-R13]

Assessing which legal ground may potentially apply under Article 7(a)-(f). Data processing can be implemented only if one or more of the six grounds - (a) through (f) - of Article 7 applies (different grounds can be relied on at different stages of the same processing activity).

[DC-D1-R14]

Qualifying an interest as 'legitimate' or ‘illegitimate’ **-** To be considered as legitimate, an interest must cumulatively fulfil the following conditions:

- be lawful (i.e. in accordance with EU and national law);

- be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently concrete);

- represent a real and present interest (i.e. not be speculative).

[DC-D1-R15]

Determining whether the processing is necessary to achieve the interest pursued - To meet this requirement, consider whether there are other less invasive means to reach the identified purpose of the processing and serve the legitimate interest of the data controller.

[DC-D1-R16]

Establishing a provisional balance by assessing whether the data controller’s interest is overridden by the fundamental rights or interests of the data subjects -

Consider the nature of the interests of the controller (fundamental right, other type of interest, public interest);

- Evaluate the possible prejudice suffered by the controller, by third parties or the broader community if the data processing does not take place;

- Take into account the nature of the data (sensitive in a strict or broader sense?);

- Consider the status of the data subject (minor, employee, etc.) and of the controller (e.g. whether a business organisation is in a dominant market position);

- Take into account the way data are processed (large scale, data mining, profiling, disclosure to a large number of people or publication);

- Identify the fundamental rights and/or interests of the data subject that could be impacted;

- Consider data subjects’ reasonable expectations;

- Evaluate impacts on the data subject and compare with the benefit expected from the processing by the data controller.

[DC-D1-R17]

Establishing a final balance by taking into account additional safeguards Identify and implement appropriate additional safeguards resulting from the duty of care and diligence such as:

- data minimisation (e.g. strict limitations on the collection of data, or immediate deletion of data after use)

- technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation')

- wide use of anonymisation techniques, aggregation of data, privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments;

- increased transparency, general and unconditional right to object (opt-out), data portability & related measures to empower data subjects.

[DC-D1-R18]

Demonstrate compliance and ensure transparency Draw a blueprint of steps 1 to 5 to justify the processing before its launch -

- Inform data subjects of the reasons for believing the balance tips in the controller's favour.

- Keep documentation available to data protection authorities.

[DC-D1-R19]

What if the data subject exercises his/her right to object? - Where only a qualified right to opt-out is available as a safeguard (this is explicitly required under Article 14(a) as a minimum safeguard):- in case the data subject objects to the processing, it should be ensured that an appropriate and user-friendly mechanism is in place to re-assess the balance as for the individual concerned and stop processing his/her data if the re-assessment shows that his/her interests prevail.

- Where an unconditional right to opt-out is provided as an additional safeguard (either because this is explicitly required under Article 14(b) or because this is otherwise deemed a necessary or helpful additional safeguard):- in case the data subject objects to the processing, it should be ensured that this choice is respected, without the need to take any further step or assessment.