C - LIST OF COMPLEMENTARY CONTEXTUAL CHECKS AND CONTROLS (CCC)

The following criteria aim at addressing technology and domain specific risks related to the processing of personal data. They complement the core criteria and shall be applied to the Target of Evaluation where applicable. "Suggested Means of Verification", including referred documents, shall be assessed against the criteria until sufficient evidences are collected to determine if the criteria are met.

Ref ID	Applicant	Specific / Generic	Level	TITLE	CRITERIA applicable to the Target of Evaluation (prescriptive clauses)	Suggested Means of Verification
C				**Complementary Contextual Checks and Controls**	Objective: To ensure that the data processing in the Target of Evaluation complies with domain-specific and technology-specific requirements	
C.1			**C**	**Public Websites Complementary Checks (where applicable)**	Condition: IF the Target of Evaluation includes a publicly accessible website, THEN:	
The use of cookies may be subject to complementary European (i.e. ePrivacy) and national rules and guidelines that shall be respected by the Applicant.						
C.1.1.1	CP	S	A	HTTPS enabled	A) HTTPS shall be enabled by default for accessing the web interface.	Inspection and test
C.4			**C**	**Video Cameras and Audio Monitoring Complementary Checks (where applicable)**	Condition: IF the Target of Evaluation includes video cameras or audio monitoring, THEN:	
C.4.1.1	C	S	A	Camera deployment validation by the DPO	A) The Data Protection Officer (DPO) or a legal expert with adequate expertise shall have checked and validated that the video camera deployment does not infringe the applicable laws and regulations for video surveillance, including the applicable national regulations.	Inspection. Video camera deployment plan and documentation. Interview with the DPO. NOCAR report.
C.4.1.2	C	S	A	Information on video surveillance	A) The Applicant shall communicate clear information to the data subjects on the areas under video surveillance through: a.1) written notice or communication to the data subjects if the video surveillance is limited to private areas whose access is limited and controlled; a.2) (OR) visible signage informing the data subject when entering in such a surveillance area.	Inspection. Documentation. Interview with the DPO.
C.4.1.3	C	S	A	Surveillance of customer space	IF video cameras are monitoring private spaces receiving visitors or customers, THEN: A) There shall be visible information that video surveillance is performed on the premises.	Inspection
C.4.1.4	C	S	A	Video network protection	A) The video cameras shall be connected: a.1) via a proprietary network protected against unauthorized access from the Internet; a.2) (OR) through end-to-end encrypted connections (i.e. IPsec in tunnel mode over IPv6).	Inspection. Sample analysis. Network documentation.
C.4.1.5	C	S	A	Access authentication to the camera	A) Cameras shall have authentication mechanisms to prevent unauthorised access with a password: a.1) larger or equivalent to 64 bits (~10 printable ASCII characters); a.2) (AND) distinct for each camera; a.3) (AND) never similar to the default password of the manufacturer. OR B) The camera shall be connected through a wire based or optical fibre based proprietary network protected against unauthorized access from the Internet.	Inspection. Sample analysis. Configuration documentation.
C.4.1.6	C	S	A	Access restriction to the video server	A) Access to the video stored on the server shall: a.1) be strictly limited to authorised employees with individual access authentication; a.2) (AND) be systematically logged.	Inspection. Sample analysis. Access logs.
C.5			**C**	**Internet of Things Deployments Complementary Checks (where applicable)**	Condition: IF the Target of Evaluation includes Internet of Things deployments (such as sensors and actuators), THEN:	
Nota Bene: Any image, biometric data, user ID, as well as data generated by mobile IoT mote that can follow the movement of natural persons or that can reveal information on data subjects activities (such as presence sensors or energy meters) shall be considered as personal data.						
C.5.1			**C**	**Complementary Checks and Controls for Internet of Things deployments**		
C.5.1.1	CP	S	A	Impact assessment complementary requirements	A) The Applicant shall have performed a Data Protection Impact Assessment (DPIA) that consider the following complementary risks for the rights and freedoms of the data subjects: a.1) the Internet of Things deployment being hacked and compromised; a.2) (AND) the IoT data being combined with other datasets that may lead to identify data subjects.	DPIA Report. PDO interview.
C.5.1.2	CP	S	A	IoT network vulnerability risk assessment	A) The Applicant shall have evaluated the risks associated to the IoT network in terms of security, including the risk that hackers use the IoT network as a weaker entry point for accessing servers where personal data are stored.	Risk assessment report
C.5.1.3	CP	S	A	IoT deployment documentation	A) The Applicant shall have an up-to-date documentation of its IoT deployment including: a.1) an inventory of all deployed IoT devices with their individual identifiers and location; a.2) network maps encompassing all deployed IoT.	Documentation review.
C.5.1.4	CP	S	A	IoT firmware updates	A) The Applicant shall have a procedure or a mechanism in place for: a.1) monitoring the need to perform secure firmware updates and patches; a.2) (AND) updating without undue delay deprecated firmware on IoT devices; a.3) (AND) using only firmware from trusted sources for upgrading the IoT devices.	Written procedures and rules. Inspection. Sample test. Penetration tests.
C.5.1.5	CP	S	A	IoT encryption	A) The transmission of personal data by IoT devices shall be encrypted.	evidence need to be produced that encryption tools are used according to the encryption policy/key management policy
C.5.1.6	CP	S	A	IoT access authentication	A) IoT nodes shall use passwords or other authentication mechanism.	Test reports Inspection

C.5.1.7	CP	S	A	Modification of "by default" passwords	A) The IoT devices shall never use a default password provided by the manufacturer.	Audit. Sample analysis Penetration tests.
C.5.1.8	CP	S	A	Least privileged principle	A) There shall be a restrictive access policy to the IoT network and data that conforms to the "least privilege" access principle.	Inspection Test
C.5.2			**C**	**Complementary Checks and Controls for Internet of Things deployed in areas accessible to the public**		
				Condition: IF the IoT devices are deployed in areas accessible to the public, THEN:		
C.5.2.1	CP	S	A	IoT area signage	A) Areas where IoT devices are collecting personal data in public space shall be signalled to the public.	Sample check and control of the presence of signage next to the IoT or where concerned persons are likely to see it.
C.5.2.2	CP	S	A	IoT transparent information	A) Data subjects shall have easy access to specific information on deployed IoT devices collecting personal data in public space, including information to contact the DPO.	Inspection. Sample test.
C.5.2.3	CP	S	B	Physical protection	A) The IoT devices shall be deployed in a manner that minimises the risk of theft.	Inspection
C.5.2.4	CP	S	B	Resilience to outage	A) The IoT devices shall be resilient to: a.1) power outage; a.2) (AND) network outage.	Inspection. Test (temporarily removing the power supply).
C.5.3			**C**	**Complementary Checks and Controls for IoT with Special Categories of Data**		
				Condition: IF the IoT devices process Special Categories of Data such as biometric or health related data, THEN:		
C.5.3.1	CP	S	B	Authentication reliability	A) To prevent unauthorised access, the authentication mechanisms shall be strong enough with: a.1) a password larger or equivalent to 80 bits (10 ASCII characters); a.2) (OR) the use of IPsec in tunnel mode over IPv6 between the gateway of the Personal Area Network and the server of the Applicant; a.3) (OR) the use of an authentication mechanism that has been assessed by independent third-parties as providing an equivalent level of reliability to a.1; a.4) (OR) the use of a wire based or optical fibre based proprietary network that has no	Inspection. Sample test and check.
C.6			**C**	**Smart Cities Complementary Checks (where applicable)**		**Sample test and check.**
				Condition: IF the Target of Evaluation is related to Smart Cities infrastructures, THEN:		
C.6.1.1	CP	S	A	Involvement of data subjects in the DPIA	The Applicant shall have involved and consulted the data subjects in the DPIA process.	DPIA report and documentation.
C.6.1.2	CP	S	A	Information of data subjects	The Applicant shall have communicated the purpose and plans related to the the smart city data processing to local data subjects.	Documentation of information communicated to the citizens. Interview of the DPO. Interview of citizens.
C.6.1.3	CP	S	A	Online information on IoT data processing	There shall be online information available to the data subjects about the smart city deployment strategy, the purpose(s) and measures set in place to protect personal data.	Website inspection.
C.6.1.4	CP	S	A	IoT devices information	The Applicant shall provide public information on the IoT devices deployed in public space by: a.1) adding labels such as QR Codes to the IoT devices; a.2) (OR) providing online information such as mobile application with a map indicating the location of the IoT devices.	Inspection. Onsite test for accessing information.
C.6.1.5	CP	S	A	Website information ease of access	The privacy policy and DPO contact details shall be accessible in no more than three clicks from the Applicant's website home page.	Website inspection
C.7			**C**	**Biometric, Medical and Health Data Complementary Checks (where applicable)**		
				Condition: IF the Target of Evaluation includes individual biometric, medical or health data, THEN:		
Nota Bene: Any data that measures physical, physiological or behavioural characteristics constitutes a biometric data.						
C.7.1.1	C	S	A	Data Protection Impact Assessment	A) The Applicant shall have performed a Data Protection Impact Assessment.	Inspection. Sample analysis. DPO interview.
C.7.1.2	C	S	B	Pseudonymisation	A) Biometric and medical data storage shall be protected by at least the use of pseudonymisation or encryption techniques (or both).	Inspection. Sample analysis. Interview of DPO and CISO.
C.7.1.3	C	S	B	Multi-factor authentication	A) Human access to the biometric, medical and health related data shall require a multi-factor authentication mechanism.	Inspection. Demonstration of Access Control.
C.7.1.4	C	S	B	Contact tracing applications restrictions	IF the target of Evaluation includes a contact tracing application, THEN: A) The application shall: a.1) require a manual activation by the user in order to start processing data and broadcasting identifiers; a.2) (AND) use pseudonymous identifiers; a.3) (AND) automatically change the pseudonymized identifier on a regular basis. AND B) The user shall be able: b.1) to know if the contact tracing application is active or not; b.2) (AND) to stop or suspend the broadcasting of its identifier.	Inspection. Tests. Technical documentation review.

C.8			**C**	**Automated Decision-making Complementary Checks (where applicable)**		
				Condition: IF the Target of Evaluation includes automated decision-making that may impact the data subjects, THEN:		
C.8.1.1	C	S	A	Test and analysis	A) The algorithm used for the automated decision-making shall have been analysed and tested in order to ensure that it is not producing discriminatory, erroneous or unjustified results.	Documentation and test report of the algorithm. Interview of the DPO, CISO or employees.
C.8.1.2	C	S	A	Written documentation from third party	IF the algorithm used is provided by a third party, THEN: A) The Applicant shall have documentation from the provider encompassing: a.1) auditing and testing carried out on the algorithm; a.2) (AND) the result of the tests confirming that it is not producing discriminatory, erroneous or unjustified results.	Documentation on the algorithm. Interview of the DPO.
C.8.1.3	C	S	A	Rights to explanations on the decisions	The Applicant shall be able to explain the decisions made by the automated decision-making to the data subject.	Sample analysis. Test. Documentation on the algorithm. Interview of the DPO.
C.8.1.4	C	S	A	Procedure for human intervention	A) The Applicant shall have rules, mechanisms or a procedure in place to enable human intervention when requested by the data subject.	Procedure and rules. Interview of the DPO.
C.9			**C**	**Blockchain and Distributed Ledger Technology Complementary Checks (where applicable)**		
				Condition: IF the Target of Evaluation includes the use of Blockchain or any Distributed Ledger Technology, THEN:		
Nota Bene: Blockchain is a specific implementation of Distributed Ledger Technology (DLT).						
C.9.1.1	CP	S	A	Data Protection Impact Assessment	A) A DPIA shall have been performed that has assessed the following complementary risks for the rights and freedoms of the data subjects: a.1) the risk that the technology prevents the data subject rights to rectify or delete their data; a.2) (AND) the risk that the technology leaks personal data with non-authorized third parties.	Documentation on Blockchain evaluation. Interview of the DPO.
C.9.1.2	CP	S	A	Compliance with effective exercise of data subject rights	A) The use of Blockchain / Distributed Ledger Technology shall not limit the exercise of the Data Subjects rights to object, rectify and delete their personal data.	Inspection. Test and demonstration of the effectivity of the data subject rights implement ability.
C.9.1.3	CP	S	A	Encryption	A) Stored personal data in the Blockchain / Distributed Ledger Technology shall be encrypted to reduce the risk of third-party access.	Inspection. Sample check and control of datasets. Interview of the CISO.
C.9.1.4	CP	S	A	Complementary check and clarification of responsibilities	A) The Applicant shall have performed a complementary analysis: a.1) to clarify the roles and responsibilities of all parties involved in the Blockchain / Distributed Ledger Technology deployment; a.2) (AND) to ensure that the Blockchain / Distributed Ledger Technology shall not transfer any personal data of the Target of Evaluation to third-parties that are not adequately acting as data processors.	Inspection. Sample check and control of datasets. Interview of the CISO.
C.10			**C**	**Data Anonymization and Pseudonymization Solutions Complementary Checks (where applicable)**		
				Condition: IF the Target of Evaluation is focused on the process of anonymisation or pseudonymisation of data, THEN:		
C.10.1			**C**	**Anonymization and risk of reidentification**		
				Condition: IF the use of anonymization technique is claimed by the Applicant, THEN:		
Nota Bene: Only data that are definitely anonymised and cannot be linked anymore (directly or indirectly) to the data subjects can be qualified as anonymised data.						
C.10.1.1	CP	S	B	Algorithm assessment	A) The Applicant shall have a report or study demonstrating that the process and algorithm used for anonymization is irreversible. AND B) The assessment of anonymization irreversibility shall have taken into account at least the following risks: b.1) to single out individuals; b.2) (AND) to link records to individuals; b.3) (AND) to infer information on individuals."	Algorithm / process analysis. Deanonymisation tests.
C.10.1.2	CP	S	B	Deanonymization check	A) IF Statistical Disclosure Control methodology is applied, THEN anonymized datasets shall be consistent and comply with the defined thresholds.	Sample analysis. Deanonymisation tests.
C.10.2			**C**	**Pseudonymization**		
				Condition: IF the use of pseudonymization technique is claimed by the Applicant, THEN:		
Nota Bene: From a legal perspective, pseudonymized data shall be treated as personal data, and should comply with the related rights and obligations.						
C.10.2.1	CP	S	B	Dissociation	A) The information required to link the data subjects with their pseudonymized data shall be protected and securely stored with distinct access rights than those for the pseudonymized datasets.	Checking the data storage location and use of distinct access rights.
C.10.2.2	CP	S	B	Access limitation	A) IF pseudo-identifiers are generated using encryption, THEN private keys shall be secured. AND B) IF pseudo-identifiers are generated using hashing function, THEN complementary measures shall be taken such as salted-hash function or keyed-hash function.	Registry of access rights. Testing the effectivity of access rights policy. Interview of employees and DPO. DPO written statement.
C.10.2.3	CP	S	B	Rectification compliance	IF the Applicant can associate pseudonymized data with the data subjects, THEN: A) The pseudonymisation technique set in place shall not prevent the exercise of the data subject rights, including: a.1) the right of the data subjects to rectify their pseudonymised data; a.2) (AND) the right of the data subjects to delete their pseudonymised data; a.3) (AND) the right of the data subjects to suspend the processing of their pseudonymised data.	Inspection and demonstration. Testing the procedure/mechanism and checking the results in the database.

C.11			**C**	**Artificial Intelligence and Data Analytics Complementary Checks (where applicable)**		
				Condition: IF the Target of Evaluation includes processing of personal data based on artificial intelligence or on data analytics, THEN:		
C.11.1			**C**	**Artificial Intelligence**		
				Condition: IF the Target of Evaluation includes processing of personal data based on artificial intelligence with a potential effect on the data subjects, THEN:		
Nota Bene: The European Commission has adopted the following definition of Artificial Intelligence (AI) in its Communication on AI:*"Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)."*A complementary definition has been elaborated by a High level panel of experts mandated by the EU: *"Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)."*						
C.11.1.1	CP	S	A	Complementary risk assessment	A) The Applicant shall have performed a Data Protection Impact Assessment encompassing the artificial intelligence mechanisms used in the Target of Evaluation, including at least the assessment of the following risks: a.1) the risk on the right to private life of the data subjects and to the protection of their personal data; a.2) (AND) the risks that decision may be taken on the basis of the AI that could negatively impact the data subjects or restrict its freedom of decision; a.3) (AND) the risk to reduce the ability of the data subject to control the use of its personal data; a.4) (AND) the risk that the data and/or the algorithms can be manipulated; a.5) (AND) the risk that the AI algorithm is subject prejudice or leads to discriminatory or unfair decisions; a.6) (AND) the risk of personal data being used for any type of social scoring, especially in regards to social media and cloud services; a.7) (AND) the risk of personal data being used by AI in any intrusive manner.	DPIA documentation. Inspection. Interview with the DPO and data subjects.
C.11.1.2	CP	S	A	Complementary informed consent	A) IF the processing is based on consent, THEN the data subjects shall have been provided with clearly and explicit information about: a.1) the use of artificial intelligence before collecting their consent and processing their data; a.2) (AND) the reasons and purpose for using artificial intelligence mechanisms; a.3) (AND) the main benefits and risks identified in the DPIA; a.4) (AND) IF the AI mechanism leads to decisions or predictions that may affect the data subjects, THEN information shall be provided to the data subjects about the procedure to access, oppose, and rectify the results of their data processing based on AI algorithms.	User interface and/or contractual documents with the data subject. Inspection. Rules, policies, procedures and mechanisms in place. Sample analysis. Testing the procedure made available to the data subjects.
C.11.1.3	CP	S	B	Record keeping	IF the Applicant provides the Artificial Intelligence solution used in the Target of Evaluation, THEN: A) The Applicant shall keep records of documentation related to the selection and/or development of the algorithm used by its Artificial Intelligence.	Documentation review. Sample analysis. Interview with the DPO and/or experts.
C.11.1.4	CP	G	B	Continuous Risk Assessment	A) The Applicant shall have rules, policies, procedures or mechanisms in place to ensure that the risks related to the use of artificial intelligence techniques are monitored and regularly reassessed. AND B) In addition to the usual risks, the risk analysis shall take into account the risk of data or algorithm manipulation.	Rules, policies, procedures and mechanisms. Risk assessment documentation. Inspection. Interview with the DPO.
C.11.2			**C**	**Big Data Analytics**		
				Condition: IF the Target of Evaluation includes big data analytics technologies OR any data processing of over 1 petabyte of data per year, THEN:		
Nota Bene: Big Data is defined as extremely large data sets that may be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions. Big Data is characterized by a large volume, high velocity of data processing and variety of processed data (the rule of the 3 Vs specified by Gartner). Additionally, in the context of Europrivacy, we consider that any data analytics that encompass over 1 petabyte of data per year shall be considered as Big Data analytics.						
C.11.2.1	CP	S	A	Complementary conformity check by the DPO.	A) The DPO or an expert with adequate expertise shall have assessed the risks of extracting or generating any categories of personal data that would exceed the declared purpose. AND B) Where mitigation measures have been identified, the Applicant shall have taken action to implement these measures.	Inspection. Dataset sample analysis. Interview of DPO and employees. Algorithm inspection. DPIA report review.
C.12			**C**	**Work Environment and Relationship Complementary Checks (where applicable)**		
				Condition: IF the Target of Evaluation is related to work environment or relationship, THEN:		
C.12.1			**C**	**Work Environment**		
				Condition: IF the Target of Evaluation relates to work environment, THEN:		
C.12.1.1	CP	G	A	Bring Your Own Device	A) The Applicant shall have written rules, policies, or contractual clauses prohibiting or framing the use of personal devices by the employees (Bring Your Own Device policy).	Rules, policies, contractual clauses. Mechanisms set in place (i.e. to restrict access to USB ports). Inspection. Sample analysis. Testing the procedure made available to the data subjects. Interview of DPO, CISO and employees.

C.12.1.2	CP	S	A	Professional devices	IF the Target of Evaluation includes professional portable devices made available to the employees, THEN: A) The Applicant shall have written rules, policies, or contractual clauses that specify the rules (or prohibition) of use of such devices for personal use, including: a.1) if the device can be used for personal use; a.2) (AND) if the data stored in the device can be accessed by the employer; a.3) (AND) if the device and its content can be accessed by third-parties; a.4) (AND) the security and access rules applicable to the device.	Rules, policies, procedures and mechanisms set in place. Contractual clauses. Inspection. Sample analysis. Testing the procedure made available to the data subjects. Interview of DPO, CISO and employees.
C.12.2			**C**	**Work Relationship**		
				Condition: IF the Target of Evaluation relates to work relationship, THEN:		
C.12.2.1	CP	S	A	DPO access and validation	A) The Applicant shall have written rules, policies, procedures or mechanisms in place to enable employees to easily contact the DPO for an question related to the processing of the personal data. AND B) The DPO or an expert with adequate legal expertise shall have assessed and validated the lawfulness, proportionality and adequacy of the employees' data processed in the Target of Evaluation.	Rules, policies, procedures and mechanisms set in place. Contractual clauses. Inspection. Sample analysis. Testing the procedure made available to the employees. Interview of DPO and employees.
C.13			**C**	**Financial and insurance services Complementary Checks (where applicable)**		
				Condition: IF the Target of Evaluation is related to financial and insurance services, THEN:		
C.13.1			**C**	**Financial and insurance services**		
C.13.1.1	CP	S	A	Supervisory Authority information	A) Where required by national law, the Applicant shall demonstrate it has informed, and where required obtained prior authorization from, its National Supervisory Authority to deliver the financial and/or insurance services in the Target of Evaluation.	Communication with the National Supervisory Authority. Interview of the DPO.
C.13.1.2	CP	S	A	Restriction of data processing	A) The Applicant shall have policies, processes or mechanisms in place to limit the data and information processed when assessing financial soundness and creditworthiness of data subjects.	Rules, policies, procedures and mechanisms set in place. Inspection. Sample analysis. Interview of DPO and employees.
C. 14				**Connected Vehicles Complementary Checks (where applicable)**		
				Condition: IF the Target of Evaluation includes Connected Vehicles, THEN:		
C.14.1.1	CP	S	A	Data processing information or documentation	A) The driver shall have access to the following information on the data processing of the Target of Evaluation: a.1) the scope and nature of the personal data processing; a.2) (AND) the purpose of its personal data processing; a.3) (AND) how to control and deactivate the personal data processing; a.4) (AND) how to access and delete the stored personal data; a.5) (AND) how to contact the Data Protection Officer (DPO) of the Data Controller.	Documentation review. Inspection. Test. Sample analysis.
C.14.1.2	CP	S	A	Vehicle usage data communication	IF usage data are communicated or remotely collected from the vehicle, THEN: A) There shall be a mechanism or a procedure in place to ensure that prior informed consent of the owner of the vehicle is collected before the transmission of such usage data.	Inspection. Tests and sample analysis. Technical documentation review.
C.14.1.3	CP	S	A	Regular processing of geolocation data	IF geolocation data are communicated or remotely collected from the vehicle, THEN: A) The DPO or a qualified expert shall have assessed and validated that: a.1) the granularity of retrieved geolocation data is not more detailed than necessary to achieve the purpose of the processing; a.2) (AND) the retention period of the geolocation data is no longer than necessary to achieve the purpose of the processing. AND B) There shall be a mechanism or process in place: b.1) to ensure that the purpose of geolocation data processing is communicated to the driver; b.2) (AND) to enable the driver to deactivate the processing of geolocation data. AND C) The user interface of the vehicle shall display an icon to inform the data subject when geolocation data are processed.	Inspection. Sample test. Documentation related to effective implementation of security measures.
C.14.1.4	CP	S	A	Special processing of geolocation data in case of theft	IF a mechanism is in place to enable the location of a vehicle in case of theft, THEN: A) The activation and deactivation of remote geolocation of the vehicle in case theft shall be controlled by the owner of the vehicle (or by a qualified national authority).	Inspection. Tests and sample analysis. Technical documentation review.
C.14.1.5	CP	S	A	Tracking via in-vehicle WiFi technology	IF the vehicle contains Wi-Fi connectivity, THEN: A) The driver shall have the possibility: a.1) to prevent the WiFi system of the vehicle to connect to external access points; a.2) (AND) to deactivate the collection and storage of IP and MAC addresses of passengers.	Inspection. Tests and sample analysis. Technical documentation review.
C.14.1.6	CP	S	A	In-car applications and processing	IF the Applicant uses an in-car application platform, THEN: A) There should be a mechanism in place: a.1) to inform the drivers on the personal data processed by the in-car applications; a.2) (AND) to enable the drivers to activate and deactivate the processing of personal data by the in-car applications. AND B) Personal data collected by the in-car applications shall not be transmitted to any third parties, except if a specific informed consent has been given by the driver. AND C) There shall be a mechanism in place enabling the owner of the car: c.1) to have access to the personal data generated by the in-car applications; c.2) (AND) to delete the personal data collected by the vehicle before the vehicle is put up to sale.	Inspection. Sample test. System analysis.

C.14.1.7	CP	S	A	Behavioural monitoring	IF behavioural data are collected from the vehicle (i.e. through a telematics box), THEN: A) The driver shall be specifically informed about: a.1) the presence of behavioural monitoring; a.2) (AND) the purpose and scope of behavioural monitoring. AND B) The raw data of the driving behaviour shall be processed or pre-processed locally (in the vehicle or on the driver's personal device) in order to minimize data exposure.	Inspection. System analysis. Sample tests. Technical documentation review.
C.14.1.8	CP	S	A	Utilization requirements of eCall system	IF an eCall system is included in the Target of Evaluation, THEN: A) The Applicant shall ensure that data subjects are provided with information on: a.1) the scope and purpose of data processing by the eCall; a.2) (AND) the retention period of data stored by the eCall system; a.3) (AND) the fact that the vehicle is not under constant surveillance; a.4) (AND) the fact that the eCall system is activated by default; a.5) (AND) the competent contact to submit a request and exercise data subject rights.	Documentation review. Inspection. Test.
C.14.1.9	CP	S	A	Securing vehicle's communications	A) The communication system of the vehicle shall: a.1) encrypt communication channels; a.2) (AND) use authentication mechanism of the devices taking part in vehicle communication; a.3) (AND) use authentication mechanism of servers authorized to perform firmware/software patches and updates; a.4) (AND) where applicable, use of frequencies allocated to vehicles communication.	Risk analysis report and documentation. Inspection. Test.
C.14.1.10	CP	S	A	Other security measures	A) The car shall include the following security measures: a.1) it shall partition the vehicle's vital functions from those relying on telecommunication capacities; a.2) (AND) it shall require user authentication to access the stored personal data; a.3) (AND) it shall include a system or solution to detect and alert in case of intrusions in the data management system of the vehicle. a.2) (AND) it shall enable remote patching of firmware and software vulnerabilities during the lifespan of the vehicle; a.5) (AND) it shall store a log history of access to the vehicle's information system.	Documentation review of security measures and technical specifications. Inspection. Sample test. System analysis.
C.14.1.11	CP	S	B	Biometric data restrictions	IF biometric data is used in connected vehicles, THEN: A) The data subject shall be able to use a non-biometric alternative. AND B) The biometric data: b.1) shall not be transmitted to a remote server; b.2) (AND) shall not be stored in clear format. AND C) The risk related to the use of biometric data in the processing shall have been assessed in the context of a Data Protection Impact Assessment (DPIA).	Inspection. Sample test. System analysis.
C.14.1.12	CP	S	B	Data processing revealing criminal offenses or other infractions	A) The Data Processing Impact Assessment shall have evaluated the risk for the data subjects that the data processing of the vehicle communicates criminal offenses or other infractions.	Data Protection Impact Assessment and/or risk analysis reports.
C.14.1.13	CP	S	B	Protection of V2X traffic and communications data	IF V2X communications are implemented, THEN: A) The Applicant shall have rules, policies, contractual clauses, guidelines, or mechanisms in place to ensure processing of traffic data is only performed by authorized entities or service providers. AND B) The applicant shall implement technical measures to: b.1) prevent the identification or re-identification of vehicles or users; b.2) (AND) minimize information disclosure to the bare minimum necessary for system operation; b.3) (AND) prevent linking of the diverse pseudonyms assigned to a vehicle; b.4) (AND) ensure that credential revocation does not affect the unlinkability of previously signed messages.	Documentation review. Inspection. Test and sample analysis.
C.15			**C**	**Smart Grid and Metering Complementary Checks (where applicable)** Condition: IF the Target of Evaluation includes smart grid or smart metering, THEN:		
C.15.1.1	CP	S	A	DPIA Extension	A) The Applicant shall have performed a Data Protection Impact Assessment (DPIA) that has taken into account at least: a.1) the risk of data subject profiling and mass surveillance; a.2) (AND) the risk of third party access; a.3) (AND) the risk of smart meter hacking; a.4) (AND) the impact on risk of the planned measurement intervals. AND B) The Applicant shall have taken measure to address the risks identified by the DPIA.	DPIA documentation review. Interview of the DPO.
C.15.1.2	CP	S	A	Data minimization by design	A) The Data Protection Officer (DPO) or a qualified expert shall have assessed and concluded that: a.1) the smart meters only transmit data that are needed to address the purpose of the processing; a.2) (AND) where applicable, the data are processed and/or aggregated locally to avoid unnecessary transfer of personal data; a.3) (AND) access to the processed data is strictly limited to the entities and users who legitimately need to access it; a.4) (AND) the data retention period is limited and justified.	Documentation review. Interview of the DPO.
C.15.1.3	CP	S	A	Privacy Enhancing Technologies (PET)	A) The Applicant shall: a.1) encrypt remote communications with the smart meters; a.2) (AND) pseudonymize data subjects identifiers; a.3) (AND) analysed and assessed the applicability of other privacy-enhancing technologies (PETs) such as masking protocols and data aggregation.	Inspection. Interview with the DPO and/or CISO. Sample test analysis. Technical documentation review.

C.15.1.4	CP	S	A	Edge processing by default	A) Where applicable, the smart meters shall avoid transmitting data that can be processed or aggregated locally.	Inspection. Interview with the DPO and/or CISO. Sample test analysis. Technical documentation review.
C.15.1.5	CP	S	A	Smart grid complementary security requirements	A) The Applicant shall implement complementary technical and organisational measures to protect the smart grid network and data processing, including: a.1) to embed authentication mechanisms in the smart meters in order to reserve remote access only to authorized systems and users; a.2) (AND) to preserve data integrity against unauthorized modifications; a.3) (AND) to enable secure remote firmware patch and updates.	Inspection. Interview with the DPO and/or CISO. Sample test analysis. Technical documentation review.
C.15.1.6	CP	S	A	Smart meters decommissioning	IF smart meters store records of consumption data, THEN: A) The Applicant shall have a procedure or a mechanism in place to ensure that stored data are systematically deleted in smart meters that are decommissioned.	Inspection. Interview with the DPO and/or CISO. Sample test analysis. Policy and procedures documentation review.
C.50			**C**	**Public Sector Complementary Checks (where applicable)** Condition: IF the Applicant is an entity part of the public sector, THEN:		
Nota Bene: Public sector includes organisations that are under the authority and effective control of public authorities.						
C.50.1			**C**	**Public Sector General Requirements**		
C.50.1.1	CP	S	A	Legitimate interest restriction	A) The lawfulness of the data processing shall not rely on a claim of legitimate interest mentioned in GDPR Art. 6 in the performance of the Applicant's tasks.	Communication with the National Supervisory Authority. Interview of the DPO.
C.50.1.2	CP	S	A	Cross-border data transfer restrictions	IF the Target of Evaluation includes potential transfer of personal data to third countries that do not have an adequacy decision and do not provide adequate safeguards for the rights and freedoms of the data subjects, THEN: A) The Applicant shall have policies, rules, or mechanisms in place to prevent such transfer in the performance of its task on the basis of: a.1) the consent of the data subject; a.2) (AND) the execution of a contract with or to the benefit of the Data Subject.	Documentation review of policies. Inspection. Sample analysis. Interview with the DPO.