Privacy Impact Assessment

PIA Title: **Liverpool Airport Consultative Committee**

Author's name: Michael Jones

Assessor's name:

Validator's name:

Creation date: 4 February 2020

Context

This section gives you a clear view of the treatment(s) of personal data in question

OVERVIEW

This part allows you to identify and present the object of the study.

What is the process under consideration?	Guidance
Membership records for Liverpool John Lennon Airport Consultative Committee and its Sub-Committees, which are gathered and kept on behalf of Liverpool John Lennon Airport by the Secretariat of the meetings, which are currently Wirral Borough Council's Committee team. The records are maintained to allow distribution of any paperwork regarding the meetings, so that further enquiries can be made when required (such as non-attendance) and to provide a simple history of membership. Occasionally, there is a need to temporarily store other data such as passport details which are required for inspection visits airside. Committee Services at Wirral Council are the Data Controller as they undertake the work of a Secretariat for the Committee, and any relevant rules will be complied with.	*Present a brief outline of the processing under consideration, its nature, scope, context, purposes and stakeholders. Identify the data controller and any processors. List the standard references applicable to the processing, which are necessary or must be complied with , not least the approved codes of conduct (see Art. 40 of the [GDPR]) and certifications regarding data protection (see Art. 42 of the [GDPR])*
What are the responsibilities linked to the processing?	
The data controller is a Principal Committee Officer and they will process data themselves or delegate it to a Committee Officer. The records will be kept solely for the purposes given above.	***Definition: Data Controller*** *Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.* *See Art. 4.7 of [GDPR]* ***Definition: Data Processor*** *Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, see Art. 4.8 of [GDPR].* *The processor and any person acting under the authority of the controller or of the processor, who has access to*

	personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law, see Art. 29 of [GDPR].
Are there standards applicable to the processing?	
?	

DATA, PROCESSES AND SUPPORTING ASSETS

This part allows you to define and describe the scope of the processing in detail.

What is the data processed?	
The data collected is contact details provided by the data subject and these are used to send out, by email or post, documents such as agenda and minutes relating to meetings, and also any additional data requested by the Airport, notably Passport details, provided by the data subject on request and required to facilitate airside visits at the airport. Details are maintained two years after leaving in case further contact is required about the person's time on the Committee and after that the name is kept so there is a record of past members and how long they have served. The data is stored in the files which are restricted to officers in Committee Services at Wirral Council and also IT administrators.	***Data and processes*** *Define and describe the scope in detail:* *- the personal data concerned, their recipients and storage durations* *- description of the processes and personal data supporting assets for the entire personal data life cycle (from collection to erasure).* ***Recipient*** *Natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. see Art. 4.9 of the [GDPR]* ***Personal data*** *Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.* *See Art. 4.1 of [GDPR]*

How does the life cycle of data and processes work?	
Once an organisation suggests an individual as their representative on the meetings, the person is contacted and asked to provide contact details. These are stored, and for meetings involving that person the details (usually just the email address) are used. Other contact details provided could be used to contact people in the case of non-attendance. Once a person leaves, the details are stored for a year in case the person needs to be contacted about an issue that took place when they were there, and after that the contact details are deleted and the name is retained for a record of membership.	Present and describe how the product generally works (from the data collection to the data destruction, the different processing stages, storage, etc.), using for example a diagram of data flows (add it as an attachment) and a detailed description of the processes carried out.
What are the data supporting assets?	
The data is stored on the shared drive of the Committee team at Wirral Borough Council, which is accessible from all of the team's secure laptops. There is no intention to ever have them on paper.	***Supporting asset*** *Asset on which personal data rely. Note: this may be hardware, software, networks, people, paper or paper transmission channels.*

Fundamental principles

This section allows you to build the compliance framework for privacy principles.

PROPORTIONALITY AND NECESSITY

This part allows you to demonstrate that you are implementing the necessary means to enable the persons concerned to exercise their rights.

Are the processing purposes specified, explicit and legitimate?	
The purpose of obtaining and processing the data is to enable the document for meetings to be shared with all of the representatives who are members. Data is provided by the representative.	**Principles relating to processing of personal data** *Personal data shall be collected for specified, explicit and legitimate purposes and* ***not further processed in a manner that is incompatible with those purposes.*** *See Art. 5.1 b) of [GDPR]*
What is the lawful basis making the processing lawful?	
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, which is acting as the Secretariat for the meetings for which the data subject is a representative.	***Justification of lawfulness*** *- The data subject has given consent to the processing of his or her personal data for one or more specific purposes* *- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract* *-Processing is necessary for compliance with a legal obligation to which the controller is subject* *- Processing is necessary in order to protect the vital*

	interests of the data subject or of another natural person *- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller* *- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child* *See art. 6 of [GDPR]*
Is the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?	
The contact data allows meeting papers to be sent to the representative, and alternative contact details (if given) can be used to contact the member if email does not work.	***Data minimisation*** *It is important to reduce the severity of the risks by minimizing the number of personal data that will be processed, by limiting such data to what is strictly necessary for the purposes for which they are processed (otherwise they should not be collected). Then, it also becomes possible to minimize the data themselves, via controls aimed at reducing their sensitivity.* ***Minimizing the amount of personal data*** *Reduce the severity of risks by limiting the amount of personal data to what is strictly necessary to achieve a defined purpose, otherwise the data shall be not collected.*
Is the data accurate and kept up to date?	
The data is only used when sending information or when there is a need to contact the person. If it was found to be wrong, it would be deleted and enquiries would be made (online or via the organisation the person was representing) to obtain more accurate information.	***Quality of data*** *Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').* *See Art. 5.1 d) of [GDPR]*
What is the storage duration of the data?	
Storage is until the information proves incorrect when the person is a member. When they cease to become a member it is maintained for a year in case of any issues which took place when the person was a member, and thereafter it is merely the name that is kept, to provide a convenient place to record prior members rather than trawl through the public minutes.	***Storage Durations*** *Storage duration must be defined for each type of data and justified by the legal requirements and/or processing needs. Thus a distinction is made between common data and archived data, to which access will be limited to only the stakeholders concerned. An erasure mechanism must be implemented to archive common data or purge archived data at the end of their storage duration. Functional traces will also have to be purged, as will technical logs which may not be stored indefinitely*

CONTROLS TO PROTECT THE PERSONAL RIGHTS OF DATA SUBJECTS

This part allows you to demonstrate that you are implementing the necessary means to enable the persons concerned to exercise their rights.

How are the data subjects informed of the processing?	
On appointment, representatives are told that their details are kept and why.	***Informing data subjects*** *Ensure that the subjects are informed. Confirm that the processing is not covered by an exception and is not subject to specific conditions.*
If consent is your lawful basis how is the consent of data subjects obtained?	
New representatives are asked to reply to approve the Code of Conduct and approve the use of their data.	***Definition: consent*** *Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. See Art. 4.10 of [GDPR]* ***Principle: Consent*** *Allow data subjects to make a free, specific and informed choice. Determine whether the processing relies on a legal basis other than consent pursuant to Art. 6 of the [GDPR]*
How can data subjects exercise their rights of access and to data portability?	
Representatives can ask about their data at any time by contacting the Secretariat.	***Right of access*** *The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information described in Art. 15 of [GDPR* ***Right to data portability*** *The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, see Art. 20 of [GDPR]*
How can data subjects exercise their rights to rectification and erasure?	

Representatives can ask to check their data at any time by contacting the Secretariat. Any erasure of vital information will result in us contacting the organisation they represent to identify a replacement representative.	***Right to rectification*** *The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.* ***Right to erasure*** *The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay, see Art. 17 of [GDPR]*
How can data subjects exercise their rights to restriction and to object?	
Representatives can ask to check their data at any time by contacting the Secretariat. Making any vital information will result in us contacting the organisation they represent to identify a replacement representative.	***Right to restricting of processing*** *The data subject shall have the right to obtain from the controller restriction of processing, see Art. 18 of [GDPR]*
Are the obligations of the processors clearly identified and governed by a contract?	
The data is processed under contract from Liverpool Airport	***Principle: Subcontracting*** *A processing contract must be signed with each processor, setting out all of the aspects stipulated in Art. 28 of the [GDPR]: duration, scope, purpose, documented processing instructions, prior authorisation where a processor is engaged, provision of any documentation providing evidence of compliance with the [GDPR], prompt notification of any data breach, etc.* ***Definition: Processor*** *Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, see Art. 4.8 of [GDPR].* *The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law, see Art. 29 of [GDPR].*
In the case of data transfer outside the European Union, are the data adequately protected?	
There will not be a need to transfer information out of the European Union.	***Transfers*** *Depending on the country in question, you will have to justify the choice of remote hosting and indicate the legal supervision arrangements implemented in order to ensure*

	adequate protection of the data subject to a cross-border transfer. That is : *- European Union* *- Country recognized as providing adequate protection by the EU* *- Transfer to the United States to a company which has joined the Privacy Shield* *- Other country* *See art. 44 to 49 of [GDPR]*

Risks

This section allows you to assess the privacy risks, taking into account existing or planned controls.

Risk Factors to consider:-

- Illegitimate access to data;
- Unwanted modification of data
- Data disappearance

PLANNED OR EXISTING MEASURES

This section allows you to identify controls (existing or planned) that contribute to data security.

#	Risk Ref	Risk Description	Mitigating Control(s)	Likely	Severity	Score
			(See details below)	**(See details below)**		
1	<Select>	Other people accessing data	Access to the files is limited to staff within Committee Services who all log in using their passwords	1	1	Select
2	<Select>			Select	Select	Select
3	<Select>			Select	Select	Select
4	<Select>			Select	Select	Select
5	<Select>			Select	Select	Select
6	<Select>			Select	Select	Select
7	<Select>			Select	Select	Select
8	<Select>			Select	Select	Select

Linked to Risk Register Information Risks

Education	Breach of IG policies and guidance due to lack of visibility, communication and training
GDPR	Non-compliant with GDPR implementation
Malware	Threat from malicious links/ attachments
Process	Information is lost/ processed in a non-compliant manner due to gaps in processes and poor controls
Purchasing	Limited governance over low spends allows DPIA process bypass
Sharing	Sharing information inappropriately or illegally due to immature technology or understanding of legislation
Supplier	Suppliers breach Privacy Law due to poor information handling practices/ IT security

Mitigating Control(s)

Logical Security Control

Encryption	Means implemented for **ensuring the confidentiality** of data stored (in the database, in flat files, backups, etc.), as well as the procedure for managing encryption keys (creation, storage, change in the event of suspected cases of data compromise, etc.). Describe the encryption means employed for data flows (VPN, TLS, etc.) implemented in the processing.
Anonymisation	Indicate here whether anonymization mechanisms are implemented, which ones and for what purpose. Remember to clearly distinguish between anonymous and pseudonymous data.
Partitioning	Implementation of data partitioning helps to reduce the possibility that personal data can be correlated and that a breach of all personal data may occur.
Logical Access Control	Methods to define and attribute users' profiles. Specify the **authentication** means implemented. Where applicable, specify the rules applicable to passwords (minimum length, required characters, validity duration, number of failed attempts before access to account is locked, etc.).
Traceability (logging)	Policies that define traceability and log management.
Archiving	Where applicable, describe here the processes of archive management (delivery, storage, consultation, etc.) under your responsibility. Specify the archiving roles (offices of origin, transferring agencies, etc.) and the archiving policy. State if data may fall within the scope of public archives.
Paper document security	Where paper documents containing data are used during the processing, indicate here how they are printed, stored, destroyed and exchanged.
Minimising the amount of personal data	The following methods could be used : Filtering and removal, Reducing sensitivity via conversion, Reducing the identifying nature of data, Reducing data accumulation, Restricting data access

Physical Security Control

Operating security	Policies implemented to reduce the possibility and the impact of risks on assets supporting personal data.
Clamping down on malicious software	Controls implemented on workstations and servers to protect them from malicious software while accessing less secure networks.
Managing workstations	Controls implemented on workstations (automatic locking, regular updates, configuration, physical security, etc.) to reduce the possibility to exploit software properties (operating systems, business applications etc.) to adversely affect personal data.
Website security	Implementation of ANSSI's Recommendations for securing websites.
Backups	Policies and means implemented to ensure the availability and/or integrity of the personal data, while maintaining their confidentiality.
Maintenance	Policies describing how physical maintenance of hardware is managed, stating whether this is contracted out. Indicate whether the remote maintenance of apps is authorized, and according to what arrangements. Specify whether defective equipment is managed in a specific manner.
Processing Contracts	Regulate the procurement relations via a contract signed intuitu personæ. - Require the processor to forward its Information Systems Security Policy (PSSI) along with all supporting documents of its information security certifications and append said documents to the contract. Ensure that the measures pursuant to its PSSI comply with the CNIL's recommendations in this respect. - Precisely determine and set, on a contractual basis, the operations that the processor will be required to carry out on personal data: 1) The data to which it will have access or which will be transmitted to it. 2) The operations it must carry out on the data. 3) The duration for which it may store the data. 4) Any recipients to which the data controller requires it to transmit the data. 5) The operations to be carried out at the end of the service (permanent deletion of data or return of the data in the context of reversibility then destruction of data at the processor's). 6) The security objectives set by the data controller. - Determine, on a contractual basis, the division of responsibility regarding the legal processes aimed at allowing the data subjects to exercise their rights. - Explicitly prohibit or regulate use of tier-2 processors. - Clarify in the contract that compliance with the data protection obligations is a binding requirement of the contract.
Network security	Depending on the type of network on which the processing is carried out (isolated, private or Internet). Specify which firewall system, intrusion detection systems or other active or passive devices are in charge of ensuring network security.
Physical access control	Policies to ensure physical security (zoning, escorting of visitors, wearing of passes, locked doors and so on).Indicate whether there are warning procedures in place in the event of a break-in.
Monitoring network activity	Monitor intrusion detection systems and intrusion prevention systems in order to analyse network (wired networks, Wi-Fi, radio waves, fiber optics, etc.) traffic in real time and detect any suspicious activity suggestive of a cyber attack scenario.
Hardware security	Indicate here the controls bearing on the physical security of servers and workstations (secure storage, security cables, confidentiality filters, secure erasure prior to scrapping, etc.).

Avoiding sources of risk	Documentation on implantation area, which should not be subject to environmental disasters (flood zone, proximity to chemical industries, earthquake or volcanic zone, etc.).Specify if dangerous products are stored in the same area.
Protecting against non-human sources of risks	Policies describing the means of fire prevention, detection and fighting. Where applicable, indicate the means of preventing water damage. Also specify the means of power supply monitoring and relief.

Organisational Control

Organisation	Specify whether a person is responsible for the enforcement of privacy laws and regulations. Specify whether there is a monitoring committee (or equivalent) responsible for the guidance and follow-up of actions concerning the protection of privacy.
Policy	Set out important aspects relating to data protection within a documentary base makingup the data protection policy and in a form suited to each type of content (risks, key principles to be followed, target objectives, rules to be applied, etc.) and each communication target (users, IT department, policymakers, etc.).
Managing Privacy risks	Policy describing processes to control the risks that processing operations performed by the organization pose on data protection and the privacy of data subjects (building a map of the risks, etc.)
Integrating privacy protection in projects	Existence of a policy designed integrate the protection of personal data in all new processing operations.
Managing personal data violations	Existence of an operational organization that can detect and treat incidents that may affect the data subjects' civil liberties and privacy.
Personnel management	Existence of a policy describing awareness-raising controls are carried out with regard to a new recruit and what controls are carried out when persons who have been accessing data leave their job.
Relations with third parties	Existence of a policy and processes reducing the risk that legitimate access to personal data by third parties may pose to the data subjects' civil liberties and privacy.
Supervision	Existence of a policy and processes to obtain an organization able to manage and control the protection of personal data held within it.

Severity Definitions

Severity	Description
Negligible severity	Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem. Examples: - physical : transient headaches - material : loss of time in repeating formalities or waiting for them to be fulfilled, receipt of unsolicited mail (e.g.: spams), reuse of data published on websites for the purpose of targeted advertising , etc., - moral : mere annoyance, feeling of invasion of privacy without real or objective harm (commercial intrusion), etc.
Limited severity	Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties Examples : - physical : minor physical ailments (minor illness due to disregard of contraindications), defamation resulting in physical or psychological retaliation, etc. - material : Unanticipated payments (fines imposed erroneously), denial of access to administrative or commercial services , Receipt of unsolicited targeted mailings likely to damage the reputation of data subjects, etc. - moral : minor but objective psychological ailments, feeling of invasion of privacy without irreversible damage, intimidation on social networks, etc.
Significant severity	Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties Examples: - physical : serious physical ailments causing long-term harm (worsening of health due to improper care, or disregard of contraindications), lteration of physical integrity for example following an assault, an accident at home, work, etc. - material : misappropriation of money not compensated, targeted, unique and non-recurring, lost opportunities (home loan, refusal of studies, internships or employment, examination ban), loss of housing, loss of employment, etc. - moral : serious psychological ailments (depression, development of a phobia), feeling of invasion of privacy with irreversible damage, victim of blackmailing, cyberbullying and harassment, etc.
Maximum severity	Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome Examples : - physical : long-term or permanent physical ailments, permanent impairment of physical integrity, death - material : financial risk, substantial debts, inability to work, inability to relocate, loss of evidence in the context of litigation, loss of access to vital infrastructure (water, electricity), etc.

	- moral : long-term or permanent psychological ailments, criminal penalty, abduction, loss of family ties, inability to sue, change of administrative status and/or loss of legal autonomy (guardianship), etc.

Likelihood Definitions

Severity	Description
Negligible likelihood	It does not seem possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in a room protected by a badge reader and access code).
Limited likelihood	It seems difficult for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in a room protected by a badge reader).
Significant likelihood	It seems possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in offices that cannot be accessed without first checking in at the reception).
Maximum likelihood	It seems extremely easy for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in the public lobby).

Risk Mapping

In accordance with the **Risk Treatment Process**

Score	Risk Class
1	Negligible
2	Limited
3	Significant
4	Maximum

		Severity			
		Negligible (1)	Limited (2)	Significant (3)	Maximum (4)
Likelihood	Maximum (4)	Medium (4)	High (8)	Very High (12)	Very High (16)
	Significant (3)	Medium (3)	High (6)	High (9)	Very High (12)
	Limited (2)	Low (2)	Medium (4)	High (6)	High (8)
	Negligible (1)	Low	Low	Medium	Medium

				(1)	(2)	(3)	(4)

Definitions

Encryption
Measure making personal data unintelligible to anyone without access authorization (symmetric or asymmetric encryption, use of public algorithms known to be strong, authentication certificate, etc.).

Anonymisation
Process removing the identifying characteristics from personal data. To assess the robustness of an anonymization processes, see the WP29 guidelines.

Pseudonymisation
Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymisation reduces the linkability of a dataset with the original identity of a data subject; as such, it is a useful security measure but not a method of anonymisation.

Data partitioning
Data organization methods that reduce the possibility that personal data can be correlated and that a breach of all personal data may occur. For instance, by identifying the personal data useful only to each business process and logically separating them.

Logical access controls
Means implemented to limit the risks that unauthorized persons will access personal data electronically, it requires among other things to :

- **Manage users' profiles** by separating tasks and areas of responsibility (preferably in centralized fashion) to limit access to personal data exclusively to authorized users by applying need-to-know and least-privilege principles.
- **Withdraw the rights of employees, contracting parties and other third parties when they are no longer authorized to access a premises or a resource** or when their **employment contract ends**.

Password
Passwords shall be composed of a minimum of eight characters; must be renewed if there is the least concern that they may have been compromised and, possibly, periodically (every six months or once a year) and must include a minimum of three of the four kinds of characters (capital letters, lower case letters, numerals and special characters); when a password is changed, the last five passwords may not be reused; the same password should not be used for different accesses; passwords should not be related to one's personal information (including name or date of birth.). Define a maximum number of attempts beyond which a warning is issued and authentication is blocked (temporarily or until it is manually unblocked).

Authentication
Every person with legitimate access to personal data (employees, contracting parties and other third parties) should be identified by a unique identifier. Choose an authentication method to open sessions that is appropriate to the context, the risk level and the robustness expected. Recommendations: if the risks are not elevated, a password may be used; however, if the risks are higher, use a one-time password token but change the default activation password, or, when part of the password is sent by SMS, a card with a PIN code, an electronic certificate or any other form of strong authentication.

Surveillance
Set up a logging architecture to allow early detection of incidents involving personal data and to have information that can be used to analyze them or provide proof in connection with investigations.

Archiving
Procedures preserving and managing the electronic archives containing the personal data intended to ensure their value (specifically, their legal value) throughout the entire period necessary (transfer, storage, migration, accessibility, elimination, archiving policy, protection of confidentiality, etc.).

Filtering and removal
When data are being imported, different types of metadata (such as EXIF data with an image file attached) can unintentionally be collected. Such metadata must be identified and eliminated if they are unnecessary for the purposes specified.

Reducing sensitivity via conversion
Once sensitive data have been received, as part of a series of general information or transmitted for statistical purposes only, these can be converted into a less sensitive form or pseudonymized. For example :
- if the system collects the IP address to determine the user's location for a statistical purpose, the IP address can be deleted once the city or district has been deduced
- if the system receives video data from surveillance cameras, it can recognize people who are standing or moving in the scene and blur them
- if the system is a smart meter, it can aggregate the use of energy over a certain period, without recording it in real time

Project Management
Measures taken to integrate the protection of personal data in all new processing operations (trusted names, guidelines, CNIL methodology for risk management or other internal methodology).

Personnal data breach
Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Reducing the identifying nature of data
The system can ensure that:
- the user can use a resource or service without the risk of disclosing his/her identity (anonymous data)
- the user can use a resource or service without the risk of disclosing his/her identity, but remain identifiable and responsible for this use (pseudonymous data)
- the user can make multiple uses of resources or services without the risk of these different uses being linked together (data cannot be correlated)
- the user can use a resource or service without the risk of others, third parties in particular, being able to observe that the resource or service is being used (non-observability)

The choice of a method from the list above must be made on the basis of the threats identified. For some types of threat to privacy, pseudonymization will be more appropriate than anonymization (for example, if there is a traceability need). In addition, some threats to privacy will be addressed using a combination of methods.

Reducing data accumulation
The system can be organized into independent parts with separate access control functions. The data can also be divided between these independent sub-systems and controlled by each sub-system using different access control mechanisms. If a sub-system is compromised, the impacts on all of the data can thus be reduced.

Restricting data access
The system can limit data access according to the "need to know" principle. The system can separate the sensitive data and apply specific access control policies. The system can also encrypt sensitive data to protect their confidentiality during transmission and storage. Access to temporary cookies which are produced during the data processing must also be protected.