Intelligent Campus

Data Protection Impact Assessment Toolkit

What's the challenge?

Different "Intelligent Campus" systems could offer a wide range of benefits, from direct assistance to students (e.g. navigation apps) to economic and governance benefits to universities and third parties. To do this a wide range of data sources and processing may be considered, from room temperature to face recognition and relationship mapping. Clearly some of these data sources are more intrusive than others.

Since data are often gathered from campus infrastructures (both physical and digital) that staff, students and visitors need to use for their education and research purposes, their support for this data gathering and use is essential. If campus occupants perceive intelligent campus applications as threatening or just creepy, they are likely to change their behaviour in ways that harm both the intelligent campus application and the infrastructures' main purposes to support teaching and research. For example if they feel they are being "tracked" students may swap access cards or passwords; staff may use mobile phone data rather than the campus wifi network.

At an early stage of the design of any intelligent campus application, the following questions need to be considered:

a) If the proposed use of sensors/data likely to be perceived as intrusive?
b) What safeguards can be applied to demonstrate safety and benefit?
c) Is the application likely to be acceptable to campus users?

Privacy Impact Assessments (PIA) are a tool designed to answer these and similar questions. These were advisory, rather than a requirement, under the European Data Protection Directive, but have now been formalised (as "Data Protection Impact Assessments" (DPIAs), with regulators using the terms interchangeably) under the General Data Protection Regulation (GDPR). The GDPR requires a full DPIA for some types of high-risk processing (see Box 1), but the approach is also useful at lower levels of privacy/data protection intrusion.

In particular, the Article 29 Working Party of Data Protection Regulators approved a PIA toolkit for Radio-Frequency ID (RFID) tags in 2011 (referred to hereafter as the "RFID Toolkit").[1,2] Since some intelligent campus systems already use RFID tags, and many others have similar characteristics, that toolkit appears a good basis for assessing the privacy/data protection impact of intelligent campus systems.

How can a DPIA help?

A Data Protection Impact Assessment shares many of the characteristics of a traditional risk assessment: in particular the need to identify risks, assess their severity, identify measures that can be used to manage them, and agree which of those measures will be adopted. However in a DPIA the risks considered are those to privacy and data protection, and the perspective taken is that of the individual whose data are processed, not that of the organisation.

Thus, for example, an information security breach might appear on a business risk assessment as a regulatory, operational and financial risk: in a DPIA it must be considered as creating a risk of harm to the individuals whose data may be accessed, modified or destroyed.

[1] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf
[2] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf

The RFID Toolkit suggests that all processes should be considered using a two-stage process:

- first an initial analysis to determine whether a DPIA is required and, if so, whether that should be small-scale or full (under the GDPR, some of the latter may be mandatory and have to meet specific legal requirements – See Box 1);
- then, if required, the appropriate DPIA itself.

For the initial analysis, the RFID Toolkit uses a four-point scale:

0) tags that are not carried by an individual;
1) tags that are carried by an individual;
2) applications that process personal data;
3) tags that contain personal data.

Level 0 applications do not require a DPIA, level 1 require a small-scale DPIA, levels 2 and 3 a full DPIA.

For Intelligent Campus applications, the definitions of these four levels can be generalised, and a fifth (level 4) added to cover the full range of applications:

0) Presence – data that is not about individuals
1) Counting – the number of individuals in a place or route
2) Identifying – individuals and/or linking to other data sources
3) Recording – so that past data can later be reprocessed
4) Analysing – data continually, e.g. face-recognition or relationship mapping.

As with the RFID Toolkit, level 0 applications do not require a DPIA, level 1 require a small-scale DPIA, levels 2 and higher require a full DPIA.

Where a DPIA is required, the RFID Toolkit provides suggestions for both the kinds of risks to individuals that should be considered, and the kinds of controls that can be used to manage them. As with the risk categories, these can be generalised and extended for Intelligent Campus applications. Once the organisation has assessed the risks and chosen controls, it can determine whether the remaining risk is likely to be acceptable to those who use the campus spaces and infrastructures.

Under the GDPR, there is strong encouragement to involve stakeholders – in particular those whose data will be processed – in this assessment: which risks are they concerned about? Which controls would they consider reasonable? Are they comfortable with the remaining risk? As noted above, for intelligent campus systems that depend on acceptance by occupants, answering these questions early in the project is a great benefit.

Mandatory DPIAs

The European Data Protection Board (EDPB) has recently endorsed the following list of characteristics likely to indicate high-risk processing.

- Evaluation or scoring
- Automated decision-making with legal or similar significant effect
- Systematic monitoring
- Sensitive or highly personal data
- Large-scale processing
- Matching or combining datasets
- Vulnerable data subjects
- Innovative use/new technical or organisational solutions
- Processing prevents data subjects from exercising a right or using a service or contract

Any processing involving two or more of these is likely to require a DPIA that satisfies the process and documentation requirements of GDPR Article 35.

Box 1 Mandatory DPIAs

Conducting a DPIA

Many documents already describe processes for conducting DPIAs. For most Intelligent Campus applications, the most relevant may be the Article 29 RFID Toolkit[3] and UCISA's PIA Toolkit;[4] for high risk applications, where a DPIA is mandatory under the GDPR and specific documentation requirements apply, it may be helpful to follow a process designed by Data Protection Regulators, for example the UK Information Commissioner[5] or the Article 29 Working Party's general approach, recently endorsed by the European Data Protection Board (EDPB).[6,7]

Whichever model is chosen, a DPIA begins by identifying the data and dataflows that are involved in an application. This information should be sufficient to conduct the Initial Analysis: Appendix 1 to this document (based on the DPIA Toolkit) sets out the likely risk levels for Intelligent Campus applications.

If the Initial Assessment concludes that a DPIA is required then the organisation should document the data and flows in detail, including the purpose and benefits, the legal basis/bases for processing and the status (data controller or data processor) of the organisations involved. Forms for recording this information are contained in each of the DPIA process documents identified above – for example Annex I of the RFID Toolkit.

The organisation should then identify the privacy and data protection risks that the data and processing may cause to individuals. Appendix 2 to this document (based on Annex III of the RFID Toolkit) suggests those that should be considered.

The organisation should then identify the controls that can be used to reduce and manage those risks. Appendix 3 to this document (based on Annex IV of the RFID Toolkit) contains suggestions.

The organisation can then determine whether the risks can be managed to an acceptable level, given the benefits that the processing will deliver. This conclusion should be documented and, if the proposal is acceptable, the controls transferred into the project plan.

[3] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
[4] https://www.ucisa.ac.uk/PIAToolkit
[5] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/
[6] http://ec.europa.eu/newsroom/document.cfm?doc_id=47711
[7] https://edpb.europa.eu/node/89

Appendix 1 – Intelligent Campus Risk Levels (derived from Article 29 Working Party RFID toolkit)

	RFID (Annex I)	Intelligent Campus
0	RFID tags unlikely to be carried by an individual	**Presence**: whether a space is occupied, including whether there are a small or large number of occupants. This could include, for example, sensing the number of wireless connection requests, the level of noise, or motion detection. No processing of identifiable information is needed, even to derive the occupancy.
1	RFID tags likely to be carried by an individual, but the application does not process or link to personal data	**Counting**: referred to as "statistical counting" in the draft ePrivacy Regulation. The canonical example is measuring queuing time by calculating how long wireless devices are stationary before moving past a bottleneck. This requires monitoring the location of individual devices over a short time period, as part of the calculation, however there is no need to link the identifiers to their users, to any other information source, or to the desired output.
2	Application processes/links to personal data, but RFID tag does not contain it	**Identifying**: including "singling out" in the Article 29 WP guidance. These applications do associate sense information with an individual, either to further link to other information sources such as their name or subject, or to provide personalised service to that individual. Human-monitored CCTV and mobile apps that are aware of their current location will generally fall into this category.
3	Application processes/links to personal data, and tag contains personal data	**Recording**: systems that record sense data for occasional later processing, for example recording of CCTV in case it is subsequently needed to investigate an incident.
4	N/A	**Analysing**: systems that involve continuous processing of sense data, such as face recognition, audio analysis for trigger words, or tracking of behaviour or relationships between individuals.

An intelligent campus can typically detect humans using three 'senses': video, audio and location. Common examples of video are CCTV and motion sensors; audio is less common, but microphones are used to monitor noise levels and may be included in some CCTV systems; location often involves mobile devices – either by external observation of their Bluetooth, WiFi or mobile phone transmissions or by devices determining their own location using sensors such as GPS – but also fingerprint readers, swipe and payment cards that are presented at particular, known, locations such as doors or shops.

While it is tempting to rank these senses by intrusiveness, as the following table shows, all three can in fact be used in both intrusive and unintrusive ways. Vision can be used to sense whether a room is full or empty, or to track individuals using face recognition; hearing can be used to measure activity in a space, or to record conversations and recognise individuals; location can provide approximate headcounts, or track an individual and their contacts throughout the day and night. Thus, when

assessing the risk from an intelligent campus application, the characteristics of the application, rather than the particular sense used, are likely to be more important. It may, however, be helpful to consider the choice of sense as a possible control measure: for example video is more likely to respect opaque boundaries such as walls.

		Sense		
		Video	Audio	Location
Risk Level	0. Presence	Motion sensor	Sound level	Wifi/bluetooth activity
	1. Counting			Wifi/Bluetooth queue monitors
	2. Identifying	Monitored CCTV		
	3. Recording	Video recording	Audio recording	Logfiles/Access Cards
	4. Analysing	ANPR/Face recognition	Voice recognition/trigger words	Relationship mapping

Appendix 2 – Intelligent Campus Risks (derived from Article 29 Working Party RFID toolkit)

Privacy Risk	**RFID Description and example (Annex III)**	**Intelligent Campus Description and example**
Unspecified and unlimited purpose	The purpose of data collection has not been specified and documented or more data is used than is required for the specified purpose. **Example**: No documentation of purposes for which RFID data is used and/or use of RFID data for all kinds of feasible analysis.	The purpose of data collection has not been specified and documented or more data is used than is required for the specified purpose. **Example**: No documentation of purposes for which intelligent campus systems used and/or use of intelligent campus data for all kinds of feasible analysis.
Collection exceeding purpose	Data is collected in identifiable form that goes beyond the extent that has been specified in the purpose. **Example**: RFID payment card information is not only used for the purpose of processing transactions but also to build individual profiles.	Data is collected in identifiable form that goes beyond the extent that has been specified in the purpose. **Example**: *Desk occupancy system collects identities of users, rather than just whether desk is free/busy*.
Incomplete information or lack of Transparency	The information provided to the data subject on the purpose and use of data is not complete, data processing is not made transparent, or information is not provided in a timely manner. **Example**: RFID Information available to consumers that lacks clear information on how RFID data is processed and used, the identity of the Operator, or the user's rights.	The information provided to the data subject on the purpose and use of data is not complete, data processing is not made transparent, or information is not provided in a timely manner. *Note that this is a particular challenge where data are collected by observation, rather than direct interaction with the individual.* **Example**: Information available to staff/students/visitors that lacks clear information on how intelligent campus data is processed and used, the identity of the Operator, or the user's rights.
Combination exceeding purpose	Personal data is combined to an extent that is not necessary to fulfil the specified purpose. **Example**: RFID payment card information is combined with personal data obtained from a third party.	Personal data is combined to an extent that is not necessary to fulfil the specified purpose. **Example**: *Wifi queue-monitoring information is combined with login records to determine location of individuals*
Multiple, incompatible purposes		*Personal data is used for multiple purposes that are neither compatible nor provided as separate options to individuals* ***Example****: Swipe card data is not only used to unlock doors, but to build study profiles of students* ***Example****: CCTV systems installed for campus security are re-used to monitor lecture attendance*
Loss of practical obscurity		*Tracking spilling into private space; private (inter)actions being captured by public sensors*

		***Example**: every student in college accommodation is tracked 24x7 through wifi usage*
Sensitive or high-risk data		*Unintentional capture of data that are either sensitive or otherwise represent a high-risk to individuals or the organisation* ***Example**: location data in counselling/medical service can reveal identities (and possibly problems, by linking to clinic timetables) of those who have been seeking help* ***Example**: video/audio of meeting rooms may capture confidential discussions/presentations* ***Example**: location data in accommodation may identify overnight visitors*
Missing erasure policies or mechanisms	Data is retained longer than necessary to fulfil the specified purpose. **Example**: Personal data is collected as part of the Application and is saved for longer than legally allowed.	Data is retained longer than necessary to fulfil the specified purpose. **Example**: Personal data is collected by an intelligent campus system and is saved for longer than legally allowed.
Invalidation of explicit consent	Consent has been obtained under threat of disadvantage. **Example**: Cannot return/exchange/use legal warranties for products when RFID Tag is deactivated or removed.	Consent has been obtained under threat of disadvantage. **Example**: *Cannot use wifi without agreeing to location tracking*
Secret data collection by RFID Operator	Some data is secretly recorded and thus unknown to the data subject, e.g. movement profiles. **Example**: Consumer information is read while walking in front of stores or in mall and no Logo or Emblem is warning him or her about RFID readouts.	Some data is secretly recorded and thus unknown to the data subject, e.g. movement profiles. **Example**: Information is collected while individual walks across campus and no Notice warns him or her about intelligent campus sensors.
Inability to grant access	There is no way for the data subject to initiate a correction or erasure of his data. **Example**: Employer cannot give employee a full picture of what is saved about him or her on the basis of RFID access and manufacturing data.	There is no way for the data subject to initiate a correction or erasure of his data. **Example**: Operator cannot give student a full picture of what is saved about him or her as a result of being present on campus.
Prevention of objections	There are no technical or operational means to allow complying with a data subject's objection. **Example**: Hospital visitor cannot opt out of reading out sensitive personal information on tags (i.e. medications).	There are no technical or operational means to allow complying with a data subject's objection. **Example**: *Student cannot opt out of video/audio observation while on campus*
A lack of transparency of automated individual decisions	Automated individual decisions based on personal aspects are used but the data subjects are not	Automated individual decisions based on personal aspects are used but the data subjects are not

	informed about the logic of the decision making. **Example**: Without notice to consumers, an RFID Operator reads all tags carried by an individual, including tags provided by another entity, and determines what type of marketing message the individual should receive based on the tags.	informed about the logic of the decision making ***Example****: Navigation app silently incorporates fitness data to send people via "healthier" routes.*
Paternalism or discrimination by algorithms		*Algorithms make decisions that are discriminatory, or should be left to the individual* ***Example****: navigation app sends user by a longer route because health data shows they should be taking more exercise*
Algorithms unaware of context		*Algorithms apply 'one size fits all' rules without awareness of external/invisible circumstances* ***Example****: Algorithm calculates that student is at risk of dropping out when, in fact, they are learning from paper books*
Decisions based on poor-quality data		*Decisions are made that do not take account of the likely (in)accuracy of the source data* ***Example****: system concludes from swipe-card data that a building is empty, when staff routinely hold doors open for one another*
~~Insufficient access right management~~	~~Access rights are not revoked when they are no longer necessary.~~ ~~**Example**: Through an RFID card, an ex-trainee gets access to parts of an enterprise where he or she should not.~~	Replaced by "Insufficient Security" below
~~Insufficient authentication mechanism~~	~~A suspicious number of attempts to identify and authenticate are not prevented.~~ ~~**Example**: Personal data contained on tags is not protected by default with a password or another authentication mechanism.~~	Replaced by "Insufficient Security" below
Insufficient data/system security		*Security mechanisms to protect data, systems and sensors do not provide adequate protection [check the GDPR wording] for the sensitivity of data or processing* ***Example****: a software vulnerability allows intruders to access CCTV cameras* ***Example****: an IoT device does not implement strong encryption, allowing information to be seen by others* ***Example****: inadequate access controls allow members of staff to see the Principal's current location*

Deanonymisation/De-pseudonymisation		*Data that is supposed to be anonymous/pseudonymous can be associated with individuals, whether using patterns, combinations of datasets or external information* ***Example**: anonymous data recorded in a student room is likely to relate to its occupant* ***Example**: Desk occupancy information combined with login information can reveal individual's working habits*
Illegitimate data processing	Processing of personal data is not based on consent, a contract, legal obligation, etc. **Example**: An RFID Operator shares collected information with a third party without notice or consent as otherwise legally allowed.	Processing of personal data is not based on consent, a contract, legal obligation, etc. **Example**: An Intelligent Campus Operator shares collected information with a third party without notice or consent as otherwise legally allowed.
Insufficient logging mechanism	The implemented logging mechanism is insufficient. It does not log administrative processes. **Example**: It is not logged who has accessed the RFID employee card data.	The implemented logging mechanism is insufficient. It does not log administrative processes. **Example**: It is not logged who has accessed the intelligent campus data.
Uncontrollable data gathering from RFID Tags	The risk that RFID Tags could be used for regular profiling and/or tracking of individuals. **Example**: Retailer reads all tags that they can see.	*Intelligent campus systems collect data about people who are neither staff nor students* ***Example**: Wifi sensors track all those on, or near, campus*
Reduced participation		*Intrusive use of sensors causes individuals to withdraw from less intrusive ones* ***Example**: A university's use of Wifi location data to profile students' study habits causes students to stop using eduroam and location-aware apps*
Perceived surveillance causes individuals to change behaviour		*Individuals who feel they are under surveillance may change what they say or do, potentially suppressing their rights to free speech & free assembly* ***Example**: Concern about 'surveillance' by CCTV causes staff to avoid sensitive topics in lectures*

Appendix 3 – Intelligent Campus Controls (derived from Article 29 Working Party RFID toolkit)

Control	RFID Description (Annex IV)	Intelligent Campus Description
Application Governing Practices	Governing practices may include: • Management practices by the RFID Application Operator. • Disposal of and erasure policies for RFID data. • Policies related to lawful processing of personal information. • Provisions in place for data minimisation in handling RFID data, where feasible. • Processing or storing of information from tags that do not belong to the RFID Operator. • Security Governance practices.	Governing practices may include: *Governing the choice of Intelligent Campus applications:* *• Policies on the definition and assessment of purposes, including Data Protection Impact Assessments where appropriate* *• Provisions to determine the compatibility of different purposes, and to offer granular choices to individuals* *• Policies on the choice of sensors/data, especially where existing sensors/data are re-purposed* *• Policies covering high-risk locations (e.g. residences, counselling services): whether IC is appropriate and if data require special treatment (e.g. reduced location precision)* *• Policies governing any data sharing (e.g. with commercial partners)* *• Provisions in place to deal with concerns or behaviour change among users of monitored spaces* Governing the design and conduct of Intelligent Campus systems: • Management practices by the Intelligent Campus system operator. • Policies related to lawful processing of personal information. *• Privacy by Design provisions, including minimisation of data collection and processing (including use of anonyms/pseudonyms), default settings (where appropriate)* • Retention, disposal of and erasure policies for IC data. *• Policies to address processing or storing of information about visitors and guests, as well as staff and students.*

		• *Governance of algorithms (relating to discrimination, paternalism, data quality, etc)* • Security Governance practices.
Providing Individual Access and Control	• Providing information about the purposes of the processing and the categories of personal data involved. • Description of how to object to the processing of personal data or withdraw consent. • Identification of process to request rectification or erasure of incomplete or inaccurate personal data.	• Providing information about the purposes of the processing and the categories of personal data involved. • Description of how to object to the processing of personal data or grant/withdraw consent for different purposes. • Identification of process to request rectification or erasure of incomplete or inaccurate personal data. • *Providing technical controls where possible, e.g. location-aware apps that individuals can choose to install/enable/disable (e.g. at particular times or in particular places)*
System Protection with respect to the appropriate protection of privacy and personal data should also be documented in this Section of the PIA Report. System protection concepts apply to back-end systems and communication infrastructure in so far as they are relevant to the RFID Application. Where they do apply, it should be recognised that backend systems are often complex and may have been the subject of their own PIA. That analysis may need to be reviewed to assure that it considered information of the nature used by the RFID Application.	• Access controls related to the type of personal data and functionality of the systems are in place. • Controls and policies put in place to ensure the Operator does not link personal data in the RFID Application in a manner inconsistent with the PIA Report. • Whether appropriate measures are in place to protect the confidentiality, integrity, and availability of the personal data in the systems and in the communication infrastructure. • Policies on the retention and disposal of the personal data. • Existence and implementation of information security controls, such as: o Measures that address the security of networks and transport of RFID data. o Measures that facilitate the availability of RFID data through	**Back-End System protection** • Access controls related to the type of personal data and functionality of the systems are in place. • Audit and system logs related to the type of personal data, functionality of the systems, and actions of their operators are in place, as well as appropriate protection for those logs from intentional or unintentional harm. • Controls and policies put in place to ensure the Operator does not link personal data in the Intelligent Campus systems in a manner inconsistent with the PIA Report (in particular to protect pseudonyms and anonyms). • *Controls and policies put in place to ensure those with access to systems and data are appropriately trained, supported and monitored* • Whether appropriate measures are in place to protect the confidentiality, integrity, and availability of the personal data in

Where no such PIA exists, the following components of the backend system should be considered:	appropriate back-ups and recovery.	the systems and in the communication infrastructure. • Policies on the retention and disposal of the personal data. • *Existence and implementation of policies for incident detection, response and notification*. • Existence and implementation of information security controls, such as: o Measures that address the security of networks and transport, storage and processing of Intelligent Campus data (e.g. encrypted communication with sensors). o Measures that facilitate the availability of Intelligent Campus data through appropriate resilience, back-ups and recovery, and well as appropriate measures to protect the security of resilient systems and back-ups.
RFID Tag Protection **RFID Tag Protection** controls related to privacy and personal data should be indicated. They are particularly relevant to RFID Applications that use RFID Tags containing personal data. Mitigation can include user based controls that address situations where different needs or sensitivities related to privacy may be at issue. Deactivation or removal are currently the two most common forms of end-user/consumer mitigation. These may either be required as part of a PIA analysis, in certain circumstances by law	• Access control to functionality and information, including authentication of readers, writers, and underlying processes, and authorisation to act upon the RFID Tag. • Methods to assure/address the confidentiality of the information (e.g., through encryption of the full RFID Tag or of selective fields). • Methods to assure/address the integrity of the information. • Retention of the information after the initial collection (e.g., duration of retention, procedures for eliminating the data at the end of the retention period or for erasing the information in the RFID Tag, procedures for selective field retention or deletion). • Tamper resistance of the RFID Tag itself. • Deactivation or removal, if required or otherwise provided	**Sensor, Device & App Protection** • Access control to functionality and information, including authentication of sensors, apps, and underlying processes, and authorisation (if appropriate) to communicate with the device/app. • Physical and logical security of sensors against unauthorised access/reconfiguration • Methods to assure/address the confidentiality of the information (e.g., through encryption of device/app). • Methods to assure/address the integrity of the information. • Methods to secure any information retained after the initial collection (e.g., duration of retention, procedures for eliminating the data at the end of the retention period or for erasing the information in the device/app, procedures for selective field retention or deletion). • Security of any app/programme/device itself.

or as a customer option after the point of sale to enhance confidence. In addition, the EC Recommendation on RFID Privacy and Data Protection for RFID Applications suggests certain methodologies and best practices associated with implementation of deactivation or removal in retail		• *Minimising the technical capability of sensors to only the functionality required (e.g. mobile app should not request access to phone functions it does not need; location-aware apps should stop tracking when not active; sound-level sensors should be disabled from acting as microphones)*
Accountability Measures These measures are designed to address procedural data protection, in the area of accountability. Through these measures external awareness regarding RFID Applications is raised.	• Ensuring the easy availability of a comprehensive **information policy** that includes: o Identity and address of the RFID Application Operator. o Purpose of the RFID Application o Types of data processed by the RFID Application, in particular if personal data are processed. o Whether the locations of RFID Tags will be monitored when possessed by an individual. o Likely privacy and data protection impacts, if any, relating to the use of RFID Tags in the RFID Application and the measures available to mitigate these impacts. • Ensuring concise, accurate and easy to understand **notices** of the presence of RFID readers that include: o The identity of the RFID Application Operator. o A point of contact for Individuals to obtain the information policy. • Noting if and how **redress mechanisms** are made available: o RFID Application Operator accountable legal entity (-ies) (may be one for each jurisdiction or operating area).	• Ensuring the easy availability of a comprehensive **information policy** that includes: o Identity and address of the Intelligent Campus Application Operator. o Purpose(s) of the Intelligent Campus Application o Types of data processed by the Intelligent Campus Application, in particular if personal data are processed *o Type(s) of data source/sensor used and how these are protected against misuse.* o Whether the locations of individuals, or their devices, will be monitored. *o Information about any automated decision-making that may be used* o Likely privacy and data protection impacts, if any, relating to the Intelligent Campus Application and the measures available to mitigate these impacts *o Link to any DPIA that has been conducted.* • Ensuring concise, accurate and easy to understand **notices** of the presence of Intelligent Campus data collection/sensors that include (at least): o The identity of the Intelligent Campus Application Operator *o The purpose(s) for which data are being collected*

	o Point(s) of contact of the designated person or office responsible for reviewing the assessments and the continued appropriateness of the technical and organisational measures related to the protection of personal data and privacy. o Inquiry methods (e.g., methods through which the RFID Application Operator may be reached to ask a question, make a request, file a complaint, or exercise a right). o Methods to object to processing, to exercise access rights to personal data (including deleting and correcting personal data), to revoke consent, or to change controls and other choices regarding the processing of personal data, if required or otherwise provided. o Other redress methods, if required or otherwise provided.	*o Any third parties with whom the information will be shared* o A point of contact for Individuals to obtain the information policy. • Noting if and how **redress mechanisms** are made available: o Intelligent Campus Application Operator accountable legal entity. o Point(s) of contact of the designated person or office responsible for reviewing the assessments and the continued appropriateness of the technical and organisational measures related to the protection of personal data and privacy. o Inquiry methods (e.g., methods through which the Intelligent Campus Application Operator may be reached to ask a question, make a request, file a complaint, or exercise a right). o Methods to object to processing, to exercise access rights to personal data (including deleting and correcting personal data), to grant/revoke consent, or to change controls and other choices regarding the processing of personal data, if required or otherwise provided. o Other redress methods, if required or otherwise provided.