Privacy-Enhancing Technologies

White Paper for Decision-Makers

Ministry of the **Interior** *and* **Kingdom Relations, the Netherlands**

December 2004

Privacy-Enhancing Technologies

White Paper for Decision-Makers

Written for the Dutch Ministry of the Interior and Kingdom Relations

Directorate of Public Sector Innovation and Information Policy (DIIOS)

Authors:

KPMG Information Risk Management

- drs. ing. Ronald Koorn RE (editor)
- Drs. Herman van Gils RE RA
- Drs. Joris ter Hart
- Dr. ir. Paul Overbeek
- Drs. Raúl Tellegen

In collaboration with John Borking

Contents

Table of Contents

1 Management summary

This White Paper on Privacy-Enhancing Technologies (PET) is written as a stimulus to apply PET for the secure processing of personal data. PET is the common name for a range of different technologies to protect sensitive personal data within information systems. PET offers the following advantages:

- PET enables processes that would otherwise be impossible;

- Privacy controls incorporated in information systems can be more effective and efficient than organisational procedures and manual actions. Processes can therefore be optimised by the application of PET;

- Utilisation of PET signals trustworthiness, and creates public confidence in the processing of their personal data in government information systems;

- The costs associated with the application of PET technology in information systems can be minimised when privacy aspects are already taken into account during the design phase of the system. Both the quantitative and the qualitative benefits of PET are considerable, for the organisations involved, for the public and for society in general.

Is PET suitable for all types of public service information systems?

Provision of public services is unthinkable without far-reaching computerisation, both within and between organisations (information supply chain). Clearly, more and more key registers are connected via back-office systems – whether or not accessible via a single front-office – to enhance customer-centric services, to reduce fraud and to improve the quality of personal data.

> PET is a suitable tool for achieving advanced types of information exchange within privacy constraints.

There appear to be PET solutions for all types of information systems. The different PET types discussed in this White Paper are: centralised database, connected back-offices, clearinghouse, information supply chains and local databases. We note that not all PET options are suitable for all types of systems.

> PET can be applied within all types of information systems.

Which PET options can be applied?

Encryption and logical access security controls are two familiar and widely used basic PET options. In the context of logical access controls, adequate management of uniquely identifying personal data and the corresponding authorisation data are particularly important.

An important PET technique concerns the separation of data in several domains. One domain contains the identifying personal data and another the other personal data. As a result, for example financial, legal or medical information is then contained in one or more domains – separate from the domain containing information on the person's identity. The data contained in each separate domain is not sensitive as it cannot be attributed to a single natural person. In this PET option, software is used to ensure that only authorised system users are able to link data from the different information domains. A different form of data separation is the introduction of a system function that only verifies the information detail that is stored in the database, but does not release the information. For example, the function only responds positively or negatively to a prompt.

All PET options have successfully been applied in operational systems.

A higher degree of integration of data and software is achieved by a PET option in which the personal data can only be accessed via specific software – the so-called privacy management system. This software enforces the privacy regulations which apply to the information system. An immediate check is performed on each data element and every system function to ensure whether a specific action complies with the privacy regulations.

The ultimate PET option concerns the anonymisation of personal data. This involves software that does not register the identifying personal data at all, or destroys it as soon as the data is no longer required – preferably immediately after collection and verification. Ideally, personal data is not stored at all. This is the maximum form of personal data protection, thus instantly complying with legal data protection requirements. Of course, it is not always possible to apply anonymisation; in situations where registration of personal data is essential, one of the aforementioned PET options would be better suited.

The figure below illustrates the PET "staircase" indicating that the effectiveness of the protection of personal data depends on the type of PET applied. The suitability of the different PET options primarily depends on the characteristics of the information system, the required level of protection and the sensitivity of the personal data concerned.

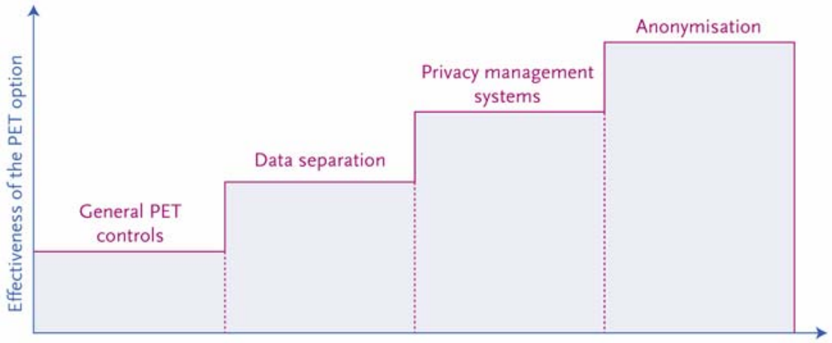

Figure 1: PET staircase

What are the costs and benefits of PET?

Three important aspects need to be considered in order to ascertain whether there is a positive business case in your organisation for applying PET:

- the one-off and on-going costs associated with the use of PET;
- cost reduction and quality improvement;
- the contribution to the business and system objectives.

In most projects, the costs of the PET application represent only a minor percentage of the overall budget and can therefore be recovered rapidly.

How can PET be applied?

An important lesson learnt from earlier PET projects is that already in the initial project stages one should consider the necessity for storing personal data, the method of data protection and the corresponding costs and benefits. This ensures that data protection is taken into account as one of the system requirements and thus naturally included in the development and implementation process. Different privacy considerations can be addressed, of which the three most important ones are:

- prevention against identification;
- protection against unlawful processing of personal data;
- the application of specific technologies to enhance privacy.

The later addition of PET to an information system is certainly possible, given some experiences in practice, but sometimes it can have further-reaching consequences for the information system. As a rule, this particularly applies to the advanced PET options and controls.

PET requirements should ideally be included at the start of a project or, in case of a major system modification, in the specification and design phase. *Privacy by design* is an important basis for the successful application of PET.

Are there any organisational implications?

With PET the safeguards for data protection are embedded in the system design, and therefore the requirements for organisational safeguards and accountability are easier to fulfil. PET has to claim its place in the product lifecycle management of information systems. This implies that, in addition to the design and implementation, attention should also be focused on privacy-related aspects, such as privacy governance, risk analysis, testing and maintaining PET controls.

An essential prerequisite for successfully implementing PET in an information system and in an organisation is that process owners, policy advisors, Privacy Officers and project managers will take PET into account as early as the initiation phase of each project.

To summarise:

PET is more than simply a means of protecting personal data:

- **PET is attractive!**
  - PET enhances the quality of information.
  - The dependence on proper compliance of processes and procedures is reduced by the automatic enforcement of privacy regulations.
  - The application of PET can offer the public better insight into and control over their personal data.

- **PET is imperative!**
  - PET simplifies compliance with data protection legislation.
  - PET provides the conditions for public confidence.
  - PET enables working with sensitive personal data in new ways.

- **PET is possible!**
  - PET has been successfully implemented on numerous occasions, which is illustrated in this White Paper.
  - PET has only a limited effect on the cost of developing new information systems, since the technologies are available and only need to be applied. The ‘cost’ mainly involves thinking and designing.
  - Implementing PET in your information architecture enables the efficient application of PET in different information systems.

Figure 2: Reasons for using PET

2 Why PET?

This section focuses on the reasons for applying PET right away, and is divided into the following paragraphs:

- PET as an opportunity for data processing which would otherwise be impossible (§ 2.1);
- Technical realisation of legal requirements (§ 2.2);
- Privacy-Enhancing Technologies (§ 2.3);
- What do I get from PET? (§ 2.4);
- Why now? (§ 2.5).

2.1 PET as a means for data processing that would otherwise be impossible

Everything points in the irreversible direction of more, more efficient and user-friendly public service provision. Examples include the ‘one-to-one’ approach in marketing and the ‘collect once, use many times’ approach practiced in government organisations, agencies and independent governing bodies. Various proposals have so far been formulated in different policy documents and programmes, such as Streamlining Key Data, Citizen and Business Service Numbers, Government Transaction Port, National Public Key Infrastructure for digital signatures and Electronic Government for Municipalities. Soon, it will no longer be possible to continue along the old lines of data processing without streamlining, integration and coordination with other government departments. Efficiency improvement and cost control will soon become important driving forces for renewal. The government has to be prepared for this. Since maintaining a high level of public confidence in the government is the key to the success of new initiatives, such as chain computerisation and e-government, a number of essential precautionary controls are essential. After all, confidence enables communication and cooperation with one another. In our tangible world, we have gradually learned, which signals inspire confidence. Often, it is a question of non-verbal body language. There are no tangible signals in the virtual world. Protecting the public’s personal data is an absolutely vital cornerstone of the policy aimed at achieving and maintaining public confidence in the government. Without that confidence, resistance to efficient and individually tailored services will grow and services will be approached with suspicion.

Frequently Asked Question (FAQ) 1: Does data protection have a stifling effect?
Organisations often experience data protection as something stifling. The reason for this is that the practical implications of personal data protection are only taken into consideration at a late stage. It then appears extremely inconvenient and inefficient to still implement PET controls at that point or even afterwards. If data protection is considered early on in a project and is included as part of the system design, it goes hand-in-hand with the functionality of the information system without any one aspect having to make concessions to another.

The ever-increasing technological possibilities mean that more and more data will be collected and stored, including detailed personal data. In most cases, data registration has a direct link with the primary process that has to be performed; however, sometimes it has a different or no clear objective at all. For instance, the amount of information people are required to fill in on the Internet if they simply want to download a document. Sometimes, name and address have to be provided, as well as additional information, such as profession or employer. Yet, this information is not required for downloading the document, but is used to create a profile of the website visitor. The government also frequently registers personal data; indeed, not with the aim of developing commercial marketing activities, but of providing a better service to the public, or simply out of habit. Especially with the rise of e-government and the reduction of the administrative burden, there is an increasing tendency to collect data electronically, whereby it is possible to obtain a particular profile of people. Studies into the protection of personal data reveal that there are potentially many unintentional risks of privacy being infringed. The easiest way around this is to compile and process only the data that are strictly necessary for the purpose for which they have to be processed; no more, and no less. Personal data protection, therefore, is in our own interest.

Domestic and international directives and legislation have been enacted in order to protect personal data, of which the European Directive on Data Protection (95/46/EU) is the most important in the context of data protection. This Directive took effect across the entire EU on 24 October 1998. It means that virtually every organisation has to satisfy the relevant statutory privacy requirements[1]. Experience shows that full compliance is no simple task as it affects large parts of most organisations.

2.2 Technical realisation of legal requirements

At present, data protection is very much centred around the legal and administrative areas, with management having to spend a lot of time on the (policy) development and monitoring. Under a lot of pressure already, management can better devote this time to other activities. Suppose that the protection of personal data could be automated more than has been the case so far: this would free-up time for the primary processes for which you are responsible. Plus, it would better enforce personal data protection. Is it possible? During the passage of the Personal Data Protection Act through the Dutch Parliament, it became clear that Information and communication Technology (IT) could play a significant role in guaranteeing the protection of personal data of citizens. Besides organisational controls such as separation of duties and data handling procedures, technology can also be deployed to protect personal data. The term ‘Privacy-Enhancing Technologies’ (PET) is used to define all the technical controls that can be used to protect personal data (see list of definitions in Appendix C for a definition of the PET concept). This concept also includes the design of the information systems architecture.

PET increases the public’s confidence, and makes it possible for the government to apply new technology to expand and improve public services.

[1] To be absolutely clear: the Data Protection Directive defines personal data as ‘*every fact concerning an identified or identifiable natural person.*’

FAQ 2: Is PET a topic for the IT organisation?

No. First of all, PET requires a policy on personal data protection; after the appropriate PET option has been selected, it is a question of correct implementation. The PET option is usually supplemented with organisational and procedural controls, such that the privacy risks are properly covered. IT staff can provide an indication of the available technical possibilities and can further design, develop and implement these after a business decision has been made. It is not essential to aim for a 100% PET solution; the crux of the matter is to protect personal data effectively and efficiently.

The Personal Data Protection Act defines the rights and duties of all the relevant organisations and people with respect to the processing of personal data. ‘Processing’ includes the entire lifecycle from collection and storage through to destruction. The Personal Data Protection Act also defines a number of basic privacy principles. The relevant principles are described in Figure 3.

1. Transparency	Prior to the first registration of data, the person concerned must be informed about the organisation’s identity and the reason for processing the data in order to consent to that processing.
2. Justification	The collected personal data are only processed if the purpose for which they were collected can be justified and if the data will not be further processed in any manner incompatible with that purpose.
3. Legitimate ground	The Personal Data Protection Act restricts the instances in which personal data may be processed. The processing of sensitive data (religion, race, health, sex life, trade union membership, etc.) is unlawful unless specific conditions have been satisfied.
4. Quality	For the purpose for which they are intended, personal data should be relevant, not excessive but proportional to the processing purposes, adequate, accurate and not kept longer than necessary.
5. Rights of the individual	The individual concerned (data subject) has the right of access, rectification, erasure, blocking and objection to processing of his or her personal data.
6. Security	The responsible party must take the necessary technical and organisational precautions to safeguard personal data from loss or against any form of unlawful processing.
7. Transfer to non-EU countries	The transfer of personal data to countries outside the EU is not permitted unless similar, ‘adequate’ privacy rules apply.

Figure 3: The essential principles of privacy

The principles of privacy listed in the figure above provide the necessary guarantees for protecting personal data. Everyone processing personal data has to bear these principles in mind and comply with the Personal Data Protection Act. However, it is not the only reason for respecting the privacy of people’s personal information. Society also expects that personal data will be protected. In this context, the government has an exemplary role in complying with the legislation it has introduced itself.

2.3 Privacy-Enhancing Technologies

From a functional perspective, it is not difficult to implement PET. With the aid of PET, it is possible to protect information about a person, such as identity and personal details. PET comprises all the technological controls for guaranteeing privacy. For instance, PET can be used to detach identification details from the other data stored about the person. The link between the identification details and the other personal details can only be restored with the use of specific tooling. Another option offered by PET is to prevent the registration of personal details altogether, for instance, once the identity has been verified. Software can also be used to enforce the condition that personal data are always disclosed to third parties in compliance with the prevailing privacy policies. The different PET options are further elaborated in section 4.

The following case study describes an example of a type of PET applied in the Higher Educations sector[2].

Case study 1: Higher Education Clearinghouse

The Higher Education Virtual Clearinghouse (named StudieLink) will service the data exchange within the higher education sector. The higher education and research partnership organisation, SURF, developed StudieLink, with the student number and another sector number being used as a unique identifier for students. The aim of StudieLink is to bring about a simple IT infrastructure, shared data definitions and streamlining of the data exchange. Thus, it is possible to realise improved and faster data exchange and ease the administrative burden. This means that administrative data can be efficiently exchanged between educational institutes, the student grants organisation, the Dutch Statistics Bureau, the Ministry of Education, Culture and Science and others.

PET application

- restrict the use of the student number that, in most cases, is identical to the tax and social security number, to the legally prescribed exchange between StudieLink (on behalf of the relevant institute) and the student grants organisation. As soon as a student enters higher education, StudieLink assigns a new sector identification number. The sector number is further used within the institute and by StudieLink. It is therefore not possible to use the student number in all kinds of administrative processes. The connection between the student number and the sector identification number is stored in a secure table;

- directly verify entered data via a secure connection with the local authorities administration system to ensure reliable data registration;

[2] This White Paper includes several case studies to illustrate the possible applications of PET. In view of the fact that the first applications of PET were in the healthcare sector, there are more case studies from this sector than from other sectors. However, the case studies from the healthcare sector illustrate PET applications that can also be used, or already have been used, in other sectors.

- apply standard and formal agreements concerning personal data processing and the protection of identifying numbers within educational institutes;
- use authentication on the basis of knowledge (personal data, student number) and ownership (code forwarded by mail), supplemented with other means, if applicable (e.g. bank card);
- divide data into three domains: student data, institutional data and grants administrative data. These domains also determine the ownership and the protection of the data (role-based access control);
- let students access and change their own personal data online.

Benefits

Such a clearinghouse can hardly function reliably and securely without the use of PET. The PET controls increase transparency and the quality of the data, and combat fraud with diplomas and study results.

In addition to the deployment of PET, it is also essential that everyone involved in data processing recognise the importance of data protection. The organisation must realise that having more personal data is not necessarily always better. Before applying PET, it is recommended to first analyse which personal data are essential for providing the service. Data minimisation is an important principle. The advantage of this principle is that personal data that are not collected and stored logically eliminate the need to be protected. Prevention is better than cure. Another advantage is that personal data that are not stored do not need to be managed. This reduces the management and maintenance effort.

The organisation’s awareness of data protection and the appropriate technological controls precedes the development and implementation of PET. Taking the time to properly consider PET improves the application of PET.

PET is an aspect of dealing with personal data protection in a more effective and efficient manner. Even if PET is not strictly required from a legal perspective, the organisation can benefit from it. The introduction of PET requires critical thinking about personal data and its protection. This approach already enhances the integrity and confidentiality of the data. PET is therefore also a tool for ensuring the ‘hygiene’ of your information system and improving the quality of the information.

The use of PET enhances the hygiene of your information systems.

2.4 What do I get from PET?

In the previous paragraph, we demonstrated that you can use PET to guarantee the protection of people's personal data. The use of PET can also enable your organisation to better prevent and manage the risks of personal data security being breached. Of course, there are also 'ordinary' privacy solutions, but they are often highly dependent on organisational and procedural controls. This means that personal data protection is only as strong as the weakest link. Numerous security and privacy audits have revealed that people often forget to apply and continue to apply the prevailing security controls consistently, or are negligent in doing so. General information security controls do not always function, leading to privacy risks. People erect thick and expensive walls around data; however, they do not prevent personal data from leaking without organisational compliance with policies and procedures. It does not exclude the risk of unauthorised access to personal data, with all the ensuing consequences.

PET can help an organisation to implement technological controls at the source, for instance a key register, and to limit the identification details to an absolute minimum. Where it is not required, identification information is not stored or it is detached from the other personal data.

Case study 2: National Central Medication Registration

The National Central Medication Registration (LCMR system) run by Prismant and IVZ is an information system that supports healthcare workers in supplying the correct dose of prescription medication to people with a drug addiction (for example, methadone). The secondary objectives of the commissioning authorities, the Dutch Ministry of Public Health, Welfare & Sport and the Ministry of Justice, include preventing theft and incorrect use of addictive substances, as well as making policy-supporting information available. The central LCMR system is fed with information about the patients, their medication and healthcare provided from the different local registration systems.

PET application

The following PET controls have been implemented in the LCMR system:

- minimise data stored centrally; limiting it to a centrally maintained reference index;
- restrict access to personal and medical information to authorised healthcare workers by means of biometrically protected smart cards and a sophisticated and granular authorisation structure. The preferred biometric type is the use of fingerprints, with four finger scans being made of each person. Thanks to the technique chosen, it is no longer possible to make a visual fingerprint of the finger scans;

- register prescriptions on the patient's smart card, thus enabling them to obtain their medication at their chosen chemist;

- anonymise the data for research purposes and for the adjustment of medicinal prescriptions.

Benefits

Through the use of the PET application, the LCMR system offers solid guarantees concerning the identity of the patient receiving the medication and of the healthcare worker using sensitive personal data. Moreover, up-to-date information can be obtained at any given time instead of only during the opening hours of the healthcare institution. Furthermore, the smart card enables patient mobility.

The biggest advantages of a structural application of PET in information systems include:

- Thanks to PET, certain types of personal data processing are allowed that would have been impossible or unlawful without PET. Without the use of PET, the personal data protection would have been inadequate, and the processing would breach the Personal Data Protection Act.
- The use of PET creates a positive image, as a result of which both your staff and your clients can be confident that your organisation treats personal data with due care. Privacy certification can further enhance that confidence. And the advantage is that the government can perform its duties and tasks with the greatest efficiency and effectiveness.
- The application of PET, together with the data minimisation principle, raises the quality of the information. This is because fewer data are processed than normal, and users only have access to information they require. In turn, it reduces the chances of personal data becoming corrupted in your organisation. Generally, the management and maintenance effort also diminishes as personal data are not processed or are processed with more care.
- You can spend less effort thinking about the protection of personal data. At the moment you stop collecting personal data, you no longer need to ask yourself continually whether you comply with the Personal Data Protection Act[3]. The advantage is that you are not required to implement various procedural controls and do not run the risk of fines or sanctions by the Personal Data Protection Authority. In instances where you have to process personal data, the process can be made 'privacy-proof'.
- PET not only ensures the protection of personal data, it also provides the tools that are required if a person wishes to gain better insight into the data kept on him or her. This in turn, improves the quality of the stored data. It is an important privacy principle and is in keeping with the desired transparency.

[3] This depends on the location of the PET solution in the information system. This will be discussed in more detail in section 4.

FAQ 3: Is PET too expensive for my organisation?

No. There are different types of PET that can be used, each with its own cost level. It is important to ensure whether the costs associated with the solution are in proportion to the risks. Even simple, but effective PET controls can substantially improve the data protection at limited costs. In section 5, we describe how you can prepare a business case for a specific PET option, looking at both qualitative and quantitative aspects.

2.5 Why now?

In times of cutbacks and in the context of the reduction of the administrative burden, the government is looking for ways to provide services as efficiently as possible. This is reflected, for instance, in the ‘collect once, use many times’ concept around key registers, such as the registers of natural persons, benefit claimants or students. The government is also digitising its services to a considerable extent, and more and more electronic registers are being deployed.

Figure 4 contains an excerpt from the 2003 Dutch Queen’s speech at the opening of the parliamentary year, showing that key registers and electronic government are strongly on the rise.

> It is the government’s aim that approximately half the existing publicly available information will also be available on the Internet in 2004, thus making the government more accessible. In addition, the public will no longer be required in the future to provide personal data to the government time and time again, but only once.

Figure 4: Excerpt from the Dutch Queen’s Speech in 2003

As a result of this increasing digitisation and centrally key data storage, the government processes more and more personal data electronically, and databases are connected, making personal data more accessible. This may be at odds with the aforementioned privacy principles. It is therefore important to strike a good balance between personal data protection and efficient and effective data processing. Providing guarantees for personal data protection should not form an obstacle to efficient and effective public services. PET can guarantee personal data protection without making excessive demands on the processing of the data. By applying PET and streamlining personal data processing, the authorities can continue to meet the high public expectations with respect to services and dealing with personal data. With PET, you are prepared for new types of processing data.

Case study 3: RINIS Clearinghouse

RINIS facilitates the exchange of data between government organisations and the social security sector via a closed EDI network. This exchange avoids the need to inform all the individual parties of changes in personal data and organisations. Organisations such as the employee insurance administrator, the Social Insurance Bank, tax authorities, various government ministries (Justice, Interior, Finance), healthcare insurance companies, the student grants administrator and other benefit agencies exchange structured (bulk) data exchange between back-office systems, for example, informing the Social Insurance Bank of new job-seeker registrations. RINIS provides the connection between numerous sectors, with the 'sector access points' being supplied with an onsite RINIS server.

PET application

Personal data are exchanged via a closed network, with the connected parties being non-repudiatable with the use of digital certificates. The following PET controls have been applied in RINIS:

- minimisation of personal data through the exclusive exchange of tax and social security numbers and message codes only;
- high degree of security through encryption of the exchanged messages, which are authorised at message level prior to dispatch and digitally signed. Unauthorised people or IT administrators do not have access to the content of the message. The encryption keys are issued and managed by a Trusted Third Party (the so-called Certification Service Provider);
- improvement of the data quality by validating the messages on the central server, thus ensuring that only authorised codes are processed. Moreover, the messages are stored for a few minutes only – to be available for resending in the event of disruptions;
- logging at message level and not of the message content, so that retrospective verification remains possible.

Benefits

The PET application in RINIS has ensured the safe exchange of messages between parties that are certain about each other's identities and about the reliability of the personal data processing. The minimisation of personal data and the central role of RINIS increase the success of the RINIS solution.

It is clear from this section that PET offers several advantages. To avoid any misunderstanding: PET is not a separate, ready-to-use component from an information system that can be added at any time (as a 'Plug & Play' solution), and it cannot always be implemented in a jiffy. To guarantee the best results, PET should be included as an integral part of both the development and the information system itself. It is therefore recommended to include the implementation of PET as part of the regular system development. The following sections explain how PET can be applied in your organisation, list the most widely used PET options, and offer a framework for preparing a business case. This is followed by a phased plan for the actual implementation of PET.

3 Application in information systems

This section sets out how to choose a suitable PET option, and distinguishes between the different types of information systems. It is divided into the following paragraphs:

- Decision factors when selecting a PET option (§ 3.1);
- Information system classification (§ 3.2).

3.1 Decision factors when selecting a PET option

First of all, when you are going to implement a new information system, functional requirements need to be specified. These requirements or specifications naturally also include the requirements for the level of personal data protection. The specifications ultimately lead to a choice for a particular architecture or structure of the information system, for example, a centrally managed database or using databases of other organisations.

An important aspect in this respect is ascertaining whether the processing of personal data:

- is essential: ‘identity-rich’;
- is essential to a limited extent: ‘identity-low’;
- is avoidable (anonymous service): ‘identity-free’.

The structure of the information system and the personal data processing requirements make functional demands on the application of PET. Using these functional demands as a basis, a PET option can be selected that best fulfils the requirements and expectations of both the authorities and the public. The procedural and organisational controls required can also be determined in this phase. Section 4 describes the PET options, and section 6 focuses on the balance between PET and organisational and procedural controls. Figure 5 illustrates the aforementioned process in a diagram. It concerns a critical part of the system development process.

A number of steps still have to be taken before coming to the functional specifications. A number of subsequent steps are then required in order to proceed from the choice for the PET option to the implementation and becoming operational of the information system. In section 7, the phased plan focuses in more detail on selecting, designing and implementing the different PET options.

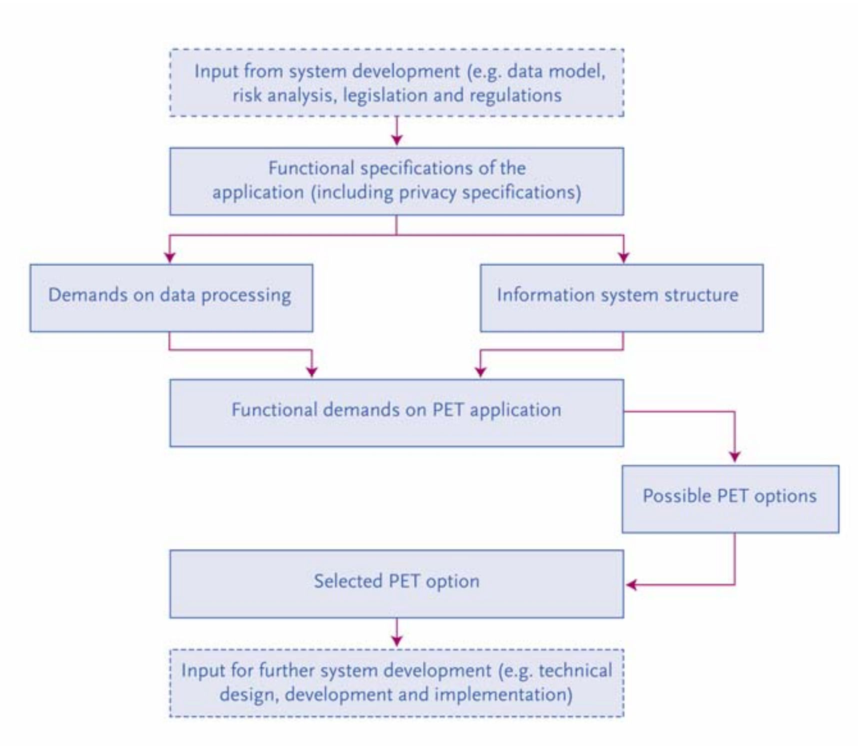
Input from system development (e.g. data model, risk analysis, legislation and regulations
Functional specifications of the application (including privacy specifications)
Demands on data processing
Information system structure
Functional demands on PET application
Possible PET options
Selected PET option
Input for further system development (e.g. technical design, development and implementation)

Figure 5: Decision factors when selecting a PET type

To support you in selecting the suitable PET option, the next paragraph, first of all, gives a brief description of the information system classification used in this White Paper. Subsequently, section 4 describes the different PET options, and makes the link between the PET options described and the different structures of information systems.

To ensure the success of PET, the development and implementation of PET must form an integral part of the system development process and must be included in the project right from the start.

3.2 Information system classification

The following information system structures are used for the purpose of this white paper:

3.2.1 Central database

In a ‘central database’ system, a single database is used for data processing. The centralised database is accessible to different people from different locations and potentially different organisations. Examples of central databases are the key registers of natural persons, companies/proprietors of the Association of Chambers of Commerce, healthcare professionals of the Ministry of Health, Welfare and Sport, student grants, benefit claimants, etc.

No data are stored or processed locally, other than directly in the central database. The processing done in the central database is initiated from one or more locations. Figure 6 illustrates the structure of the central database.

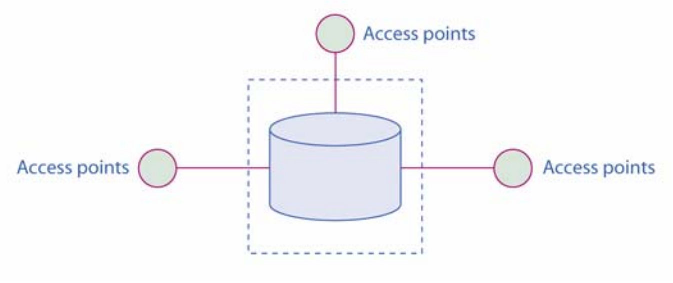

Figure 6: Central database

The case studies in this White Paper that use a central database are the LCMR system (case study 2), the LADIS system (case study 9), the X/Mcare system (case study 12) and the digital medical history file (case study 14).

3.2.2 Connected back-offices

In the structure of connected back-offices, the databases of a number of back-offices are accessed through a single front-office. A person uses a single portal to access data from different organisations. The back-offices are also connected to one another to enable access to data in numerous databases. An example is the connection between the key registers of student grants and of natural persons at a municipal level. Using this connection, the student grants organisation can validate if students are indeed registered in the place of residence they reported in order to determine whether they are eligible to receive a grant for a student living on his own or with his parents.

The connections between the back-offices can be temporary. For example, a central database can be connected to a back-office of another organisation temporarily. In addition, one of the back-offices can also serve as key register. Figure 7 illustrates the structure of the connected back-offices.

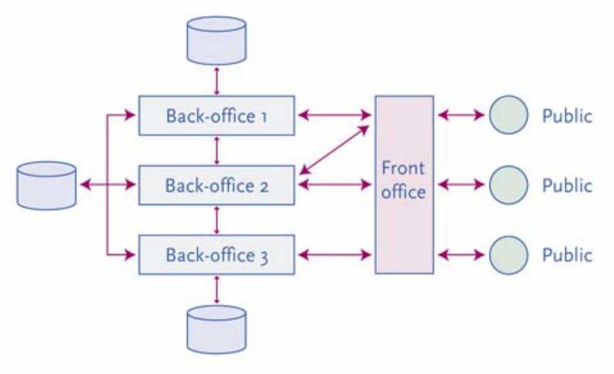

Figure 7: Connected back-offices

The case studies in this White Paper that refer to back-offices are the NTIS system (case study 4), the Suwinet (case study 5) and the Alberta system (case study 11).

3.2.3 Clearinghouse

A clearinghouse or routing organisation is the central point in the communication between and with the connected organisations. The information exchange between the connected organisations also takes place via the clearinghouse. Other institutions can only exchange information with the connected organisations via the clearinghouse. The public generally has no direct contact with the clearinghouse, but only with the other agencies connected to it.

The clearinghouse usually does not store any critical information on a permanent basis; it merely serves as an intermediary. In order to ensure effective and efficient information exchange, reference indices in the databases of the connected organisations are used for a cross-reference or routing database. Another possibility is to work with central or sector reference indices or identification numbers, such as the Citizen Service Number and and Business Service Number. Figure 8 illustrates the structure of a clearinghouse.

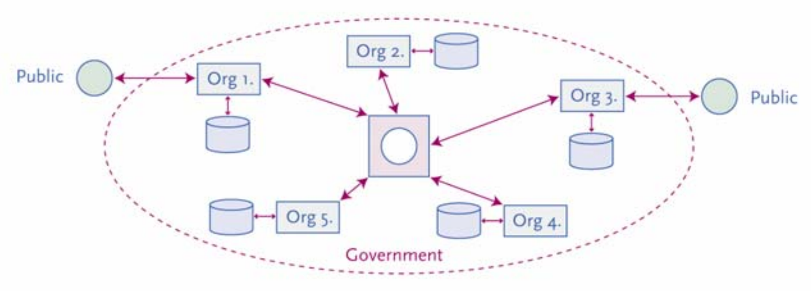

Figure 8: Clearinghouse

The case studies in this White Paper that use a clearinghouse are the Higher Education Clearinghouse (case study 1), the RINIS system (case study 3) and Suwinet system (case study 5).

3.2.4 Information supply chain

In a ‘public service chain’, information are exchanged or forwarded between a minimum of two organisations. One feature of a chain is that the supply chain organisations have their own databases for storing data. An example is the motor vehicle registration chain. Here, the connected organisations in the chain (often garage owners or motor vehicle testing centres) communicate with the Motor Vehicle agency via a communication provider. The providers collect part of the information, which the connected organisations send via them to this agency. Other examples of chains with a high level of information exchange can be found in the healthcare sector, the transport sector (e.g. data exchange in Rotterdam port) and in the (criminal) investigation process within the Police – Justice relationship (e.g. electronic reporting, charges and files). Figure 9 represents a simplified structure of the chain.

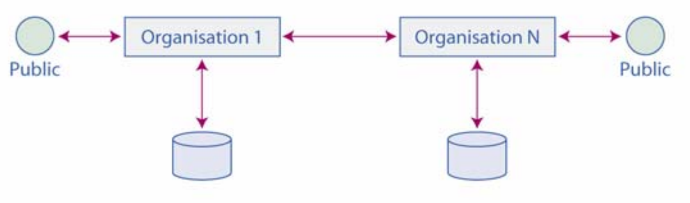

Figure 9: Chain

The case study in this White Paper that involve a system chain is the NTIS system, in combination with the information systems to be connected in the future (case study 4).

3.2.5 Local databases

In this structure, the information are spread across different decentralised databases, with the possibility of the central front-office/back-office having its own database. The local databases do not contain the same information, and the front-office/back-office does not contain the same data as the local databases. The local databases only contain the same type of information; databases from different organisations are not connected. Another example of local databases is the use of electronic smart cards, with individuals managing their own information.

Examples of local databases include the key register of natural persons at municipal level, the public transport smart card, the digital tachograph (with each lorry being fitted with a local register for tracking driving and resting times; see also § 4.4), and the solution for road pricing (kilometre charge; see also § 4.4). Figure 10 illustrates the structure of a system with local databases.

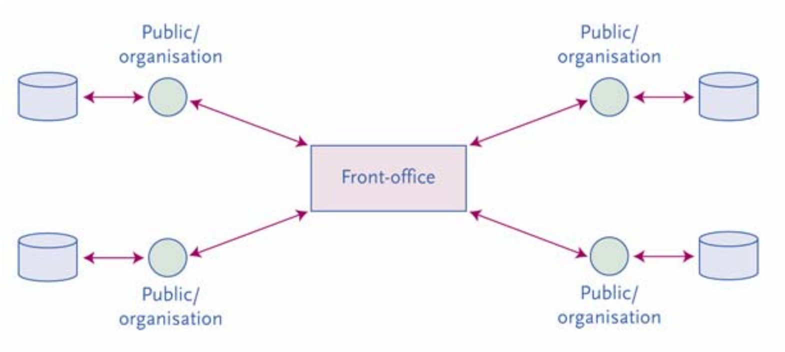

Figure 10: Local databases

The case studies in this White Paper that use local databases are the digital tachograph (case study 7), the AgeKey (case study 8), electronic voting (case study 10) and the public transport smart card (case study 13).

4 PET options

The paragraphs below describe the functioning of the different possibilities offered by PET[4], which concern the following four main types:

- general PET controls (§ 4.1);
- separation of data (§ 4.2);
- privacy management systems (§ 4.3);
- anonymisation (§ 4.4).

We then look at how an organisation can use logging and control to confirm that the implemented PET controls function properly. In addition, this section includes a PET staircase, in which the different PET options are compared to one another from the perspective of effectiveness. Finally, a link is made between the PET options described and the information system structures discussed in section 3.

4.1 General PET controls

Advantages:

- General PET controls are relatively simple to implement.
- The correct combination of general PET controls can achieve an effective basic level of personal data protection.

Many organisations apply general security controls, such as encryption and logical access security. When correctly applied, these general security controls also have a privacy-enhancing function. An example is a user gaining access to a specific data set on the basis of his/her job or tasks in the organisation. It is not necessary for every user to see the entire database. For instance, someone processing address changes does not have to see the rest of the personal data. Based on his/her tasks, the person in question is only authorised to process the address information. The task is therefore linked to the type of actions the person is authorised to perform.

[4] The reading list in Appendix A includes documentation with additional information about the different PET options.

Data minimisation

In addition, there are a number of techniques that can be used to transform data such that the identity cannot be derived. When a user does require personal data, but not necessarily the identifying details, some of these details can be removed. Another option is to remove part of the data from a database field, for example, the last three digits from the postal code, leaving the unique address unidentified, but with the receiver still having an indication of the geographical area. When, however, the entire collection of data is required, but not the exact value of a database field, it will suffice to categorise the data. For instance, if a user needs to know whether someone has attained the age of majority, the application does not reveal the age or the date of birth, but merely responds with yes or no. The user's question is thus answered, but the system user does not know the exact age of the person in question. If the user does not need to know the exact value of a field, the bandwidth of the recorded data can be expanded. For example, a random figure can be added to the age.

In a chain structure, data minimisation can also be used in the form of data filtering, with successive parties in the chain receiving less and less personal data, or with different degrees of filtering being applied to the different types of parties. In this way, only one party, or no party at all, can compile a complete profile of a person. A practical application is described in the public transport smart card case study (nr. 13).

The combination of a number of these data minimisation techniques appears to achieve fully anonymous data processing; however, this is not the case. Full anonymisation is dealt with in § 4.5.

Case study 4 concerns an example of the PET application used by the National Trauma Information System (NTIS). In addition to the general PET controls, NTIS also separates the data within the organisation. This second type of PET is dealt with in § 4.4.

Case study 4: National Trauma Information System (NTIS)

NTIS is an electronic register for emergency patients with critical injuries who are treated in the accident and emergency department. Doctors, nurses and assistants have access to this system. Electronic registration and exchange of medical information can offer the patient more efficient and effective cure and care. Highly sensitive medical information and treatment methods are also analysed anonymously so that treatment methods can be improved, the patients can be treated better and the chances of survival can be improved.

PET application

- strong security by means of a sophisticated authorisation structure, with the role of the user determining which part of the system and database the user has access to. Authorised healthcare workers use digital certificates stored on smart cards (for the most sensitive functions containing biometric information as their unique identification). Other users use software certificates, which do not provide access to the medical information;

- data separation, with the medical information and the name and address details being stored in different database tables. The name and address details are encrypted, so that unauthorised users (such as system administrators) cannot reduce the medical information to an individual natural person. The database is stored at a so-called Trusted Third Party (TTP), with stringent physical and logical access security controls. These security controls are audited on a periodic basis;

- minimisation of information that are exchanged with other information systems. Information from NTIS is transferred to a system, from which the regional medical officer can see who in his/her district has been involved in a disaster. Only a classification code is supplied in addition to the name and address details. The classification code provides information about the nature of the injury, but the regional medical officer does not gain insight into the medical information. This system has a temporary database, and the name and address details are not stored permanently in the system. However, in the current version the officer can export the data to his/her personal computer.

Benefits

The application of PET has finally made it possible to develop this system, without which the quality of the treatment offered by the accident and emergency centres will be less. Following its regional success, NTIS is currently being rolled out throughout the Netherlands and forms the basis for the nation-wide key register of trauma patients.

Authentication and authorisation

A prerequisite for most of the different PET options is that the authentication and authorisation procedures function reliably. The different PET options rely strongly on authentication and authorisation management (a.k.a. Identity Management). If due care is not taken when granting and issuing authentication means (e.g. password, token, digital certificate), unauthorised users can gain unlawful access to personal data. This would completely counteract the advantages offered by PET.

Quality-Enhancing Technology

Part of PET is a similar concept, Quality-Enhancing Technology (QET). With the aid of QET, it is possible to monitor and improve the quality (complete, accurate and up-to-date) of the data registered. The quality of the personal data strongly affects the quality of the services the government provides. What’s more, it also serves the privacy principle concerning quality (see section 2), because correct decisions can be taken when the personal data is reliable. These techniques can also be applied to remove redundant information from databases and to improve the quality of the data.

Case study 5: Suwinet

Suwinet was set-up to improve cooperation in the work and income domain of social security. For this cooperation, the social security partners, the employee insurance administrator, the Social Insurance Bank, the Centres for Work and Income and the municipal social services departments must have access to their respective data. At present, more than 18,000 employees of these agencies are connected to Suwinet. By using the information already available at these agencies, it is not necessary to ask the public or the organisations to provide information anew. Strong security and privacy conditions apply to the information exchange among the parties connected. This is specifically laid down in the relevant legislation. Suwinet is usually used in the front-office (e.g. service desk), in contrast to RINIS (case study 3), which is used in the back-office.

PET application

In addition to general security controls, such as the use of a closed, virtual private network, the following privacy safeguards were added:

- minimisation of the set of personal data exchanged for the relevant purpose. When information is required about the status of a passport, the only information that is fed back is whether the passport is (in)valid, and not the reasons for it (e.g. theft). There is also no central data storage or processing, so that administrators have no insight;
- detailed authorisation of users through the application of organisational roles even a direct connection between the type of question and the personal data to be requested (and the order of showing). The parties have no additional authorisations on the back-office systems of the other parties, and the connected parties can apply further filtering and restricting requests for sensitive personal data. Free search options are not allowed;
- improvement of the information quality by means of online enquiries and by ‘confronting’ the public at the service desk with information from other institutions in order to remove inconsistencies and maintain reliable information. This information quality is further guaranteed by the user surveys and the IT and privacy audits carried out on an annual basis both centrally and at the connected agencies;
- the requested data are logged for each staff member by tax and social security number, and not the content of the messages. This log is only accessible to authorised IT or forensic auditors. Advance statistics are also kept for each role and profile with the use of heuristic technology in order to reveal any irregularities in the data processing.

Benefits

The on-line exchange of personal data was subject to stringent privacy rules in the design of the Suwinet, where it is clear that restrictions apply to the exchange of someone’s personal data between government organisations. One-off registration, structured information exchange and the individual right to check this information all improve the quality of the personal data.

General PET controls remarks:

- Personal data are still processed.
- General PET controls mainly concern identification, authentication, authorisation and encryption.
- General PET controls are very suitable for use in combination with specific PET controls.

4.2 Separation of data

Advantages:

- Identifying data are detached from the other personal data.
- The effect does not depend on general security controls.
- It is possible to exchange personal data between organisations with due consideration for data protection.

Separation of data means that personal data are processed, but that identifying personal data are detached from the other personal data. At least two domains are created: one identity domain in which, for example, the name and address details are processed, and one or more pseudo-identity domains in which other information, such as membership or other sensitive data, is processed. The separation between the two domains is achieved and managed by an identity protector.

In practice, an identity protector is a software component that can be placed on the server. A smart card can also serve as identity protector, but this is not essential. The identity protector converts the real identity into a pseudo-identity, usually by applying identification codes that cannot be reduced. The connection between the two identities can only be re-established with the aid of the identity protector. People with authorisation to use the identity protector can gain access to both domains and see the relationship between them. People who do not require access to all the personal data to perform their tasks only have access to the pseudo-identity domains to which they are entitled.

To summarise, the identity protector has the following functions:

- generating a pseudo-identity on the basis of a real identity;
- connecting the pseudo-identity with the real identity. The two domains can be connected if the processing requires it;
- converting one pseudo-identity into another pseudo-identity. Through frequent use of one and the same identity, it is possible to discover the real identity. When different pseudo-identities are used, it is impossible to identify a pattern in the activities performed on the basis of the pseudo-identity

Given the important functions of the identity protector, it is absolutely essential that it be used with due care. Therefore, the authentication and authorisation of people is a critical process for guaranteeing the functioning of the identity protector. Authentication, for instance, can be based on a digital certificate.

In many instances, different types of users use an information system, and every user is only allowed to access a limited amount of personal data. In such a case, different pseudo-identity domains can be created, with part of the information about a person being processed in each domain.

Figure 11 illustrates the above-mentioned identity protector in a simple diagram.

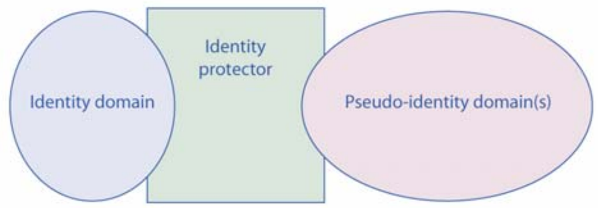

Figure 11: Separation of data

Case study 6: Identity protector in a hospital information system

To guarantee patient privacy, the patient data can be divided into two domains. The personal data, including the patient number, are stored in the identity domain. The diagnostic and treatment details are stored in the pseudo-identity domain, in which a patient number is used. The patient numbers in the two domains are not allowed to be identical, as everyone could then make the connection. To resolve this problem, the patient number from the identity domain is encrypted. The encrypted number is used as patient number in the pseudo-identity domain. The encrypted patient number can be decrypted with the aid of the identity protector and the connection can be made with the identity domain. This means that only people who are authorised to use the identity protector can make the connection between the two domains.

If an organisation wishes to conduct a statistical investigation, there is usually no need to register the identity of the individual citizens, even though the organisation wants to use data related to individual citizens. In that case, it will suffice to process the data from the pseudo-identity domain. Individuals personally control the identity protector and, thus, the connection between the two domains. This form of data separation can be used if the government requires certainty about someone’s identity, but does not wish or is not allowed to record the data. This is the case, for instance, with electronic voting (see case study 10). If people wish to vote electronically, the government has to ascertain that the person in question is entitled to vote and votes only once; however, it is absolutely essential that the identity of the voter in relation to the vote is not registered in order to safeguard the required anonymity of the vote.

This PET application can also be used the other way round. The government only registers the identity domain and only the individual has access to the pseudo-domain. In this instance, too, the individual in question decides whether the government can and is allowed to make the connection between the two domains. It should be noted, though, that for instance, a smart card has limited storage capacity and cannot store an entire collection of data (besides other risks of local storage). In many instances, the smart card will include a reference to the location where the collection of data is stored or the organisation that has stored the data. An example of this is that an individual does not personally carry an electronic patient record, but the name of the GP is stored on the smart card. In the event of an accident, the doctor in charge can contact the GP to obtain information on a person's medical history.

As a rule, the successful PET implementation usually depends on a reliable authentication and authorisation process. It is clear, for instance, that the identity protector can only function properly if the required authentication tool (e.g. a smart card) is issued to the relevant users with due care. Furthermore, correct authentication and authorisation management also offers the organisation advantages in the field of general information security and efficiency, and helps the organisation to be in control of data processing.

Personal data under personal control

Maximum data protection is achieved if the person whose data are registered controls the identity protector. That person alone determines when and to whom his/her real identity is revealed. The situation where the individual concerned controls the identity protector is known as 'personal data under personal control' and is, in fact, a specific form of separation of data. Examples include a personal smart card and an online data safe. In the aforementioned case study, the doctor in the hospital can ask for the patient's smart card to gain access to the patient's electronic medical file. It offers a high level of security, but is impractical in its implementation, because the doctor in question can only consult a patient's medical records in the presence of the – conscious – patient. The doctor, therefore, will also need to have a smart card to gain access to the medical file. Ideally, the smart card is not issued by the hospital itself; it is not specialised to do so, and there is a risk that an unauthorised person does get hold of a smart card. It is therefore advisable that a trusted third party issues the smart cards. This party is specialised to do so and identifies the system user in accordance with the prevailing authentication requirements.

Case study 7: Road Pricing & Digital Tachograph

When road pricing is used, the government registers personal data to charge for road use. The government does not need to know where and when the road user drove; it only wants to know how much to charge the user. To this end, the user has a smart card in his/her vehicle that automatically keeps a detailed register of the journeys travelled. When the road user passes a read-out post, the cumulative information on the card is registered. The authorities now know how much to charge, but only the road user has access to the details of the journeys.

A similar PET application – soon to be used on an EU-wide scale – is found in the digital tachograph, with the driving and resting times in a lorry being registered on a smart card. Additional options have been created so that the driver can have the database on the smart card signed electronically, and to offer supervisory bodies special access possibilities.

FAQ 4: What is the difference between data protection by means of logical access security and the identify protector?

Although logical access security is an important tool to prevent unauthorised access to personal data, its use does have restrictions. A disadvantage of regular logical access security is that the data are still identifiable and are stored together, usually in a single database. Other limitations are that the data can also be accessed by circumventing the application, and the fact that, often, insufficient user profiles are defined in the applications. The latter means that people often have extensive access privileges.

With the identity protector, the personal data are detached from the remaining data. Only the identity protector can make the connection between the different domains. The big difference is that the data are not processed and stored in a form that is immediately identifiable. The advantage is that if the general controls are breached and someone gains access to the different domains, it is not possible to make the connection between the personal and the remaining data. The identity protector, therefore, offers better privacy protection than the general logical access security controls.

A common difference between information security and the application of PET lies in the different points of departure. Information security primarily focuses on the increasing protection of an ever-increasing collection of data. PET, on the other hand, focuses specifically on collecting fewer data, thus requiring fewer impenetrable walls to protect the data. An application such as electronic voting, for instance, is not possible using general information security, whereas it is possible with the application of PET.

Points of attention:

- Security of the identity protector is vitally important.
- The separation of data in an existing information system often requires a thorough review of the data model.

4.3 Privacy management systems

Advantages:

- Transparency is increased for the public.
- Compliance with the privacy regulations is technically enforced.

Privacy management systems that ensure automated enforcement of the privacy policy represent a special form of PET. It concerns software that, in fact, forms a shell around the personal data and that automatically tests all transactions involving these data against the privacy regulations. This test is based on electronic privacy policies derived from the privacy regulations for the database or information system. The privacy policies are entered in the PET software by means of a privacy code or privacy language.

An operational example is the Platform for Privacy Preferences Project (P3P), designed by the World Wide Web Consortium (W3C). P3P[5] is a tool for communicating the privacy preferences of the Internet user in a simple and standardised way and in a format that the information system can read. P3P contains the following information:

- who collects, processes and stores the data;
- what data are collected and the reason for their processing;
- whether there are *opt-in* and *opt-out* alternatives;
- whom the data are supplied to;
- which data the responsible person has access to;
- the default storage period for the relevant personal data;
- how conflicts about the privacy policies of the processing organisation are resolved or settled;
- where the privacy policy can be found on the website.

[5] See http://www.w3.org/P3P/ en P3P and Privacy – Centre for Democracy & Technology / IPC Ontario – see http://www.cdt.org/privacy/pet/p3pprivacy.shtml.

This significantly increases the transparency of data processing for the user. The Internet user completes an online questionnaire, indicating his/her preferences concerning data protection. With every subsequent visit to the website, the user can automatically ascertain whether the organisation's privacy regulations respect his/her preferences and decide, on the basis of this knowledge, whether or not to visit the website. Incidentally, a similar application can be used for applications that do not run via the Internet, but that use Internet technology[6].

Practical tools are now available for defining electronic privacy language (or 'privacy ontologies'), such as the Enterprise Privacy Authorisation Language (EPAL). Various suppliers have now also developed privacy management systems or are in the process of doing so. These systems enforce compliance with the defined privacy policies during processing. First of all, the organisation's agreed privacy policies are entered in the privacy management system; then, they are integrated into the processes. When a new process and data are entered, an automatic analysis takes place to ascertain whether the process is covered by an agreed standard or rule derived from the privacy policies. An assessment is also made to ascertain whether the processes of the different organisational units are consistent. The functionalities can also be expanded to include the external processors[7], *opt-in* management and automated compliance.

Experience abroad (see also case study 11 from Canada) shows that privacy management systems substantially increase public confidence, as well as management's insight into the processing and controlling of data processing. Automated compliance in particular is a major plus and avoids costly privacy audits on organisational compliance.

Privacy management system remarks:

- The applicable technologies are recent developments and are not yet widely applied.
- One can also implement similar PET controls oneself at database level by using current products.

[6] For example, the use of the Internet TCP/IP protocol within the organisation or via virtual private networks between organisations.

[7] A third party to whom the data processing or part thereof is outsourced by the organisation responsible for the personal data registration.

4.4 Anonymisation

Advantages:

- After full anonymisation, personal data are no longer processed and no security controls are required any longer for privacy reasons.
- Less data are registered and need to be managed and maintained.

Anonymisation can be applied in two phases of data processing. In the first instance, the need for governmental agencies to register personal data of the public can be prevented, in which case no personal data are processed at all. This solution is only possible if the processing of personal data is not required for the purpose of the public service provided.

Secondly, if personal data are required temporarily, the data can first be processed and then destroyed or detached from the other data. The destruction and/or detachment of the data must be irreversible. If that does not happen, the personal and the other data can be linked again, which means that full anonymity has not been achieved. If the data have also been stripped of indirect identification features, no personal data are left whatsoever.

The advantage of anonymisation is that data that are not stored do not require management and protection. This reduces the management and maintenance effort. Furthermore, the Data Protection Act no longer applies because no personal data are being processed. Destruction and/or detachment is an option if, for example, statistical analyses have to be performed where identification data are not required or are not allowed to be processed. An anonymiser is a technical tool, for example a software program that is used to filter away the personal information of someone using IT services.

Case study 8: Anonymous services: AgeKey

The government wants to discourage smoking and has prohibited the sale of tobacco to young people under the age of sixteen. However, enforcing this prohibition proved to be a problem, for which the AgeKey was developed. The AgeKey can be stored on a bank card or smart card. Cigarette vending machines only operate if someone has such an AgeKey. To get hold of an AgeKey, a person has to go to the post office and prove that he/she is over sixteen years of age. The AgeKey is then activated on the card, and the person can buy cigarettes from the vending machine. All the vending machine does is to check whether the card contains the AgeKey; the purchase transaction is totally anonymous. No register is kept of activated Age Keys, No one knows who has an activated AgeKey or how the AgeKey is used. See www.agekey.nl for additional information.

Case study 9: National Alcohol and Drugs Information system

The National Alcohol and Drugs Information System (LADIS) is a register which keeps track of the scale and content of support provided to people with an addiction throughout the Netherlands. All the organisations in the Netherlands that provide care to people with addictions forward information to the LADIS system via a diskette or secure e-mail, on the basis of which policy information is prepared and epidemiological research conducted. Since 1994, 150,000 individuals have been registered anonymously in LADIS. There are countless users of the LADIS data; in addition to the institutions themselves, the users vary from government agencies to pharmaceutical companies, media companies, manufacturers of gambling machines, casinos and embassies.

PET application

- use of unique codes based on the personal data, with the name, gender and date of birth, among other things, being encrypted. The software used by the providing organisation produces the code, and is certified to do so. After the data transfer, the unique code is converted into a second anonymous code (by means of so-called hashing), with the original data no longer being reducible;
- safe delivery of the data through the use of encryption and password security;
- immediate destruction of the data provided by the institution.

Benefits

As a result of the over 10 years of application, LADIS has created an anonymous client tracing system. Because of the privacy controls that have been implemented, LADIS is, in fact, no longer a personal data register, making it possible to provide data to a broad target group for policy and research purposes. Despite a certain error margin (client code more than 90% unique) caused by the unsophisticated structure of the privacy-enhancing technology developed in 1994, the data can still be used for research by means of an automated correction function. It is actually possible to correct the unsophisticated structure.

Anonymisation remark:

- Anonymisation can only be applied in identity-low and identity-free processes.

4.5 The PET staircase

The description of the four PET options shows that each has specific functions related to data protection. The one option offers better protection than the other. In figure 12, the different PET options are positioned in relation to the effectiveness of the data protection. The diagram also shows the most important features of the different PET options. The PET staircase is not a growth model and does not have to be followed to the top. Once an organisation has applied general PET controls, it does not mean that it has to go on to ‘higher’ levels of PET. The suitability of the different PET options depends on the specific situation.

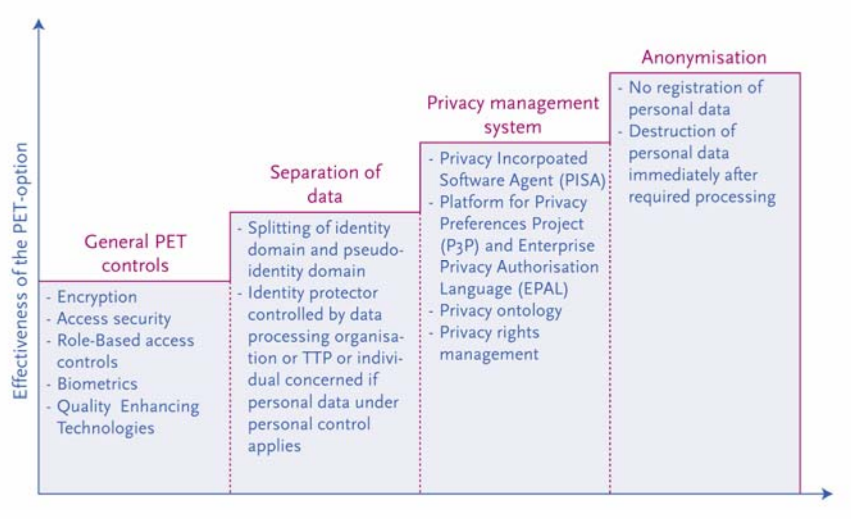
Effectiveness of the PET-option
General PET controls
- Encryption
- Access security
- Role-Based access controls
- Biometrics
- Quality Enhancing Technologies
Separation of data
- Splitting of identity domain and pseudo-identity domain
- Identity protector controlled by data processing organisation or TTP or individual concerned if personal data under personal control applies
Privacy management system
- Privacy Incorpoated Software Agent (PISA)
- Platform for Privacy Preferences Project (P3P) and Enterprise Privacy Authorisation Language (EPAL)
- Privacy ontology
- Privacy rights management
Anonymisation
- No registration of personal data
- Destruction of personal data immediately after required processing

Figure 12: PET staircase: the effectiveness of the different PET options

4.6 Connection of PET options to the information system structure

Figure 13 illustrates which PET controls can be used in which structure. It also focuses on the features of each combination at a high level. The description of the different PET options in this section and the features listed in the table provide sufficient insight into how the different PET options can be applied in the different structures.

The application of the general PET controls and the privacy management systems are not dealt with in this table, because these options can be generically applied to the different information system structures. Subsequently, the 'Personal data under personal control' sub-category is discussed separately.

	Anonymisation	Separation of data
Central database	■ Anonymisation before data are registered in database if no personal data are required; or ■ Register data temporarily and anonymise data after processing in database.	■ Both the identity domain and the pseudo-identity domain in the central database; ■ Authorised user gains access to personal data through authentication to identity protector in central database.
Connected back-offices	■ Anonymisation to front-office if connected back-office requires no personal data; or ■ Anonymisation after processing in back-office if some back-offices temporarily require personal data. Connected organisations are responsible for anonymisation.	■ Both the identity domain and the pseudo-identity domain(s) in each back-office; ■ Authorised user gains access to personal data through authentication to identity protector in back-office database.
Clearing-house	■ Anonymisation by routing organisation if connected organisations require no personal data; or ■ Anonymisation after processing by connected organisations if the latter temporarily require personal data. Connected organisations are responsible for anonymisation.	■ Both the identity domain and the pseudo-identity domain(s) at every connected organisation; ■ Authorised user gains access to personal data through authentication to routing organisation.
Information Supply Chain	■ Anonymisation by first organisation in the chain if other organisations in the supply chain do not require personal data; or ■ Anonymisation after processing by one of the chain organisations if this and following organisations do not require personal data. The supply chain organisations are responsible for anonymisation.	■ Both the identity domain and the pseudo-identity domain(s) at every supply chain organisation; ■ Identity domain at one organisation and pseudo-identity domains at other supply chain organisations; ■ Authorised user gains access to personal data through authentication to identity protector in the database of each supply chain organisation to which access is required.
Local databases	■ Not applicable since individuals personally control the data.	■ Already achieved in the central database since the individual personally controls the data.

Figure 13: Connection of PET options with the information system structure

The ‘Personal data under personal control’ PET option is a sub-category of ‘Separation of data’ and has therefore not been included in the table separately. However, there are a number of differences in the applicability of both options. These are:

- The ‘Personal data under personal control’ option is not easily applicable in connected back-offices, clearinghouses and supply chains. Due to the nature of the data processing, it is currently not yet possible, for example, to give the public control over their personal data in the entire services chain. This would actually require a software solution that protects the personal data against unauthorised processing in several registration locations at the same time and thus, in fact, travels along with the personal data. To this end, all the systems in the relevant chain have to deal in exactly the same way with the personal data controlled by the individual personally.
- In the central database, the identity domain is controlled by the individual in question, and the pseudo-identity domain is located in the central database (or vice versa). An authorised user gains access through authentication to the identity protector of the individual.
- In the local databases, the individual controls the identity domain and the pseudo-identity domain. An authorised user gains access through authentication to the identity protector of the individual.

FAQ 5: Is PET only suitable for processes in which no identity is used?

No. It is a misunderstanding that PET can only be applied in identity-low processes. It would severely hamper the applicability of PET. An identity protector, for instance, can be located at the data entry and processing end of the information system. If it is essential for the identity to be known at the start and the end of the process, it is often not the case for the intermediate internal processes. PET can be used to protect the data in these intermediate processes.

4.7 Points of attention

4.7.1 Logging and monitoring

With the aid of logging and monitoring, it is possible to confirm retrospectively that the PET controls have functioned properly. To this end, it is important to log and verify every action or every set of actions with respect to personal data that take place under the responsibility of the competent person. One example is to log at individual level the organisations to which data have been provided (including why, what and when). This creates an audit-trail (who did what and when), which means that it is possible to verify the actions and ascertain whether the PET controls function properly.

Since logging and monitoring is a means for checking whether data protection controls are complied with, it is always applied in combination with one of the other PET options. The analysis of the log files could lead to 'leaks' in the PET option being discovered and remedied. Thus, logging and monitoring also contributes to preventing unlawful processing of personal data.

A further advantage of logging and monitoring is that the rights of the individual registered can be met. An individual is entitled to ask an organisation to provide the information that is registered about him/her and to whom this information has been disclosed. With the aid of the log files, the organisation can demonstrate that the information has not been passed on at all, or that the information has only been transferred to authorised agencies or individuals.

Obviously, it is essential that the log files cannot be manipulated, thus enabling unauthorised users to delete evidence. In addition, the security officer or the data protection officer, for instance, has to review the log files on a regular basis, and regularly has to prepare reports for management (see also § 6.2). An important point for attention with respect to logging and monitoring is that the log files obviously also have to be PET-proof. One should be careful that the log files do not contain personal data, the processing of which is exactly what one tries to prevent with the use of PET.

Case study 10: Electronic voting

Politically, it has been decided that it should be possible to vote remotely and electronically. This makes it possible for Dutch citizens to cast their vote at a random polling station in the Netherlands or even abroad. Electronic voting concerns voting by telephone or via the Internet, with the public having the flexibility to make that choice at the last minute.

PET application

The law makes stringent demands on electronic voting; in response, the following PET controls have been taken:

- detach the possibility to vote from the actual voting. To this end, a separation was made between voter registration (at the municipality), enabling voting by means of the polling card (at the electronic voting organisation) and the cast vote (at the voting service of a trusted third party). A division was also made in the printing process between the production of the list of candidates and that of the personalised access codes;

- strict security of the access and voting codes used. With the aid of one-way encryption, the voter's access code is converted into a non-reducible code ('hash') that can be used to ensure that someone votes only once. The cast vote is not stored on the voter's computer. In addition, the database of the 'electronic ballot box' is encrypted with cryptographic technology such that only officials authorised by the mayor can decrypt it. A large number of candidate codes are linked to a single candidate to prevent a vote from becoming known through monitoring or tapping the connection;

- guarantee the integrity of the data. Here, transaction mechanisms are applied that ensure that a voting action can only be carried out as an entire action;
- during the voting process, actions and events are logged to enable the supervisor to monitor the voting progress retrospectively;
- destruction of voting codes and cast votes some days after the voting (once the election result becomes irrevocable);
- in-depth audits of the entire process, printers, electoral service and the software code of the electoral service prior to and around the election day/period.

Benefits

With the application of the PET controls, a cast vote is completely anonymous and cannot be reduced to the individual voter. Moreover, the voter is unambiguously and uniquely identified before casting his/her vote. The voting process is also transparent to the public, the polling station and the organisation in charge, without too many concessions having to be made to the security and the reliability of the process.

FAQ 6: Is it still possible to detect fraud after PET has been applied?

It remains possible to detect fraud after the application of PET. As shown by the description of the different PET options, there is only one option in which the data processing is completely anonymous. In that case, it is more difficult to detect fraud. When applying general PET controls and electronically enforcing compliance with the privacy policies, a person’s identity is processed and relatively simple to retrieve. The basic principle in separating data is that the identity is detached from the other data. Fraud detection, therefore, is basically not possible. When fraud is suspected, the identity protector can be used to retrieve someone’s real identity. The use of the identity protector in fraud investigations, however, must happen under strict conditions and supervision, otherwise data protection is jeopardised and public confidence will rapidly decline.

5 The business case for PET

Insight into the costs and the quantitative and qualitative benefits is essential for the decision-making process concerning the application of PET. This section focuses on:

- Desirability of PET (§ 5.1);
- Business case elements (§ 5.2);
- How do I arrive at a positive business case? (§ 5.3).

5.1 Desirability of PET

The sections above presented an operational qualification of the different PET options. A number of possibilities for the application of PET in an organisation were also presented on the basis of the different information system structures.

Three key questions have to be answered to determine whether there is a positive business case for applying PET in your organisation. These questions are:

1. Does PET make an essential contribution to the objectives of the organisation?
2. What quantitative and qualitative benefits can PET achieve in our organisation?
3. Which investment and structural costs does PET involve?

If the responses to these questions lead to the conclusion that the application of PET in your organisation is desirable and rational from a cost-benefit perspective, then the business case for applying PET is positive. The positive business case serves as the commercial justification for applying PET. The term ‘business case’ also refers to its elaboration in a decision-making document, which will serve as the primary justification and reason for including PET activities in the overall project. During the implementation, the business case will also serve as a communication means concerning the reasons for the project and as confirmation of the agreement about the net benefits to stakeholders. In this context, it is also important to describe the assumptions in reasonable detail.

Developing the business case is not an on-off task; it has to be monitored during the implementation phase (‘benefits realisation management’). During the course of the project, more insight will be gained into the benefits to be realised and the costs to be incurred. The business case has to be assessed periodically to see whether it is still positive and to adjust the project where needed.

This section offers support for preparing the business case for PET and provides building blocks for further elaboration during the execution of the project.

5.2 Business case elements

5.2.1 Policy

The most important consideration when preparing the business case is the extent to which a contribution will be made to the organisation’s policy objectives. In practice, this consideration will often be decisive and, as such, forms the cornerstone of the business case. The most important advantages described in section 2 can serve as the starting point for determining whether PET contributes towards the organisation’s policy objectives. If such a contribution is identified, the cost-benefit analysis can proceed. The key question is whether these contributions offset the costs involved. If no real contribution is made, the preparation of the business case can be stopped. If the protection of personal data is absolutely essential – for example, electronic voting in parliamentary elections – excessive costs can even ruin the entire project.

5.2.2 Benefits

The benefits offered by PET can be quantitative or qualitative. If the application of PET leads to a reduction in costs, then the benefits can be controlled and, therefore, are quantitative. Qualitative benefits are tricky to control and – by definition – hard to express in monetary terms; however, they can surpass the quantitative benefits. One example is the positive image resulting from the application of PET. Another qualitative benefit is that PET enables collaboration and data exchange between different organisations that would otherwise not be possible without the use of PET. This increases the quality of the public service, which is very difficult to express in monetary terms. Figure 14 presents a summary of the potential benefits.

Qualitative benefits	Quantitative benefits
■ PET enables applications that would otherwise be impossible; ■ Creates a positive image as perceived by the public. As a result, public confidence in the government and its electronic services is increased, which is essential for the success of this service channel; ■ Complies with the Data Protection Act; ■ Increases personal control over personal data; ■ Improves the quality of the information; ■ Strengthens the innovative image of the organisation that uses PET; ■ PET and the associated privacy management system ensure that risks of privacy breaches remain manageable.	■ Increases client satisfaction; ■ PET makes it possible to connect databases, streamline the data processing and guarantee privacy. Public services and the corresponding data processing therefore become more efficient and the administrative burden can be reduced; ■ Requires fewer personal data to be entered, corrected and processed; ■ The use of PET means less reliance upon procedural/organisational controls. This reduces the burden on the organisation and provides more certainty on data protection; ■ Makes it possible that the Internet can be used for communication purposes instead of more costly fixed connections (leased lines) and networks; ■ Reduces audit, supervisory and management costs and possible fines by Data Protection Authorities and other supervisory bodies; ■ Reduces the costs for providing information to individuals registered.

Figure 14: The benefits of PET

Not being able to quantify the benefits should not stand in the way of a positive business case. The qualitative benefits can, in fact, be very important for the success of the services and, thus, be decisive.

Business case for the National Trauma Information System

The present trauma system would not have been possible without the implementation of PET. In order to keep the costs low and manageable, the Internet had to be used. The use of the Internet automatically means that stringent data protection controls had to be applied.

5.2.3 Costs

This paragraph contains a summary of the cost items that can be used when preparing the business case. Firstly, figure 15 presents an overview of the percentage PET costs in relation to the total project costs of developing a system. Interviews with people who have been involved in the development of a PET-enabled system reveal that PET costs represent between 1 and 10% of the total project costs.

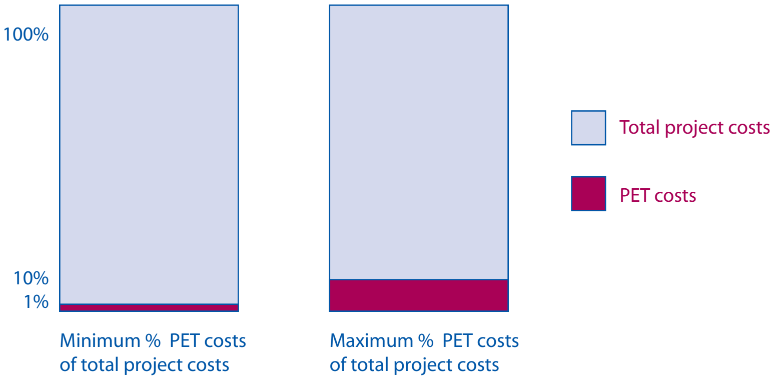

Figure 15: Percentage PET costs in relation to total project costs

The fluctuation is caused by the fact that the costs depend on the selected PET option. The accent in data anonymisation lies on the one-off investments and less on the structural costs. For example, there is no need for rolling out costly authentication tools, and the costs of the general security controls are also reduced. Personal data are no longer processed, which means that the data protection requirements can be less stringent[8].

[8] From the perspective of availability, for instance, it could very well be necessary to maintain a higher level of security.

When data are separated, different domains are created, the data model usually has to be modified, and there is more often a need for customisation to implement the PET option. When data are anonymised, the data model and the implementation are simpler, precisely because no personal data are processed. There are also more standard solutions available for anonymisation.

The costs of the general PET controls vary because of the wide range of possible controls. Encryption, for instance, is less expensive than the application of PKI-based smart cards protected with biometrics.

To get a picture of the breakdown of the specific PET costs, the costs are divided into the categories of development, rollout and management & maintenance. Development and rollout are one-off categories, and management & maintenance is a structural category. Figure 16 illustrates an estimate of the relationship between the three categories. Together, the three categories represent the total PET costs, where it should be noted that the precise ratios can differ for the different PET options and application.

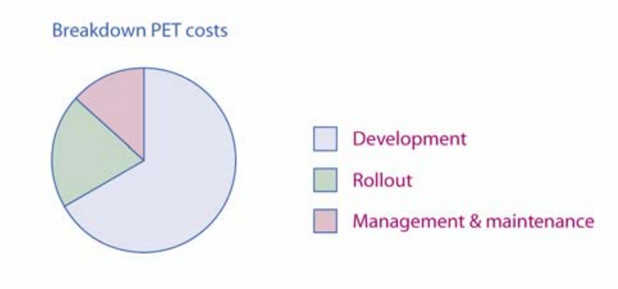

Figure16: Breakdown of the total PET costs

Figure 17 gives an indication of the cost items comprised by the aforementioned categories. This overview does not include general costs for each IT project, such as a feasibility study and functional design of the information system; it only shows PET-specific costs. In addition, a scale of low/medium/high is used to indicate the weight of each cost item in relation to the overall PET-specific costs.

	Cost category	Weight in total PET costs[9]
One-off	**Development**	
	Assessment personal data processing need	Medium
	Design data model	High
	Functional design PET option	Medium
	Technical design PET option	Medium
	Possible modifications to (technical) infrastructure	Low
	Development PET option or purchase of PET product[10]	Low – High
	Development or purchase of logging & monitoring tool	Low
	Rollout	
	Training users / administrators	Low
	Rollout of authentication tools (if applicable)	Low – Medium
	Communication[11]	Low – Medium
Structural	**Management & maintenance**	
	Management any authentication tools (if applicable)	Low
	Maintenance specific PET option	Low – Medium

Figure 17: Overview of the specific PET costs

[9] It is not possible to provide an exact estimate of the different cost items on the basis of the interviews and our limited research.

[10] The PET option can vary from simple to complex; e.g. the application of tokens or biometrics involve relatively high costs compared to a solution at the database level or with role-based access controls.

[11] In this instance, communication is seen as PET-specific as PET may change the precise way of working for the system users. It is therefore also vital to create sufficient support within the user community.

When using this overview, please bear in mind that it is a generic overview that needs to be adapted to the specific features of your organisation and the structure of the information system (see section 3).

Professor Boasson (University of Amsterdam, Road Pricing): 'The most time and investment are taken up by the design of the data model. It is one of the most important steps in the entire development process.'

Suwinet Director Kinkhorst: 'To achieve safe information exchange in the social welfare sector, we used a closed network and a sophisticated role-based access control structure. Based on the current size of the user group, the costs for this application amount to some 10% of the total costs'.

Van Blarkom, the system architect in charge of the development of one of the first-ever PET applications (for a psychiatric hospital): 'The cost of a new PET-proof hospital information system with electronic patient files only adds a small percentage to the total costs, provided proper attention is paid to PET when the system is built.'

The fact whether PET is applied to existing systems or systems in development also affects the costs. When PET is implemented in existing systems, the costs are higher than they would be in new systems. The reason is that most PET cost items are one-off costs, and the one-off activities form part of the overall system development project. When the PET-specific activities are carried out afterwards, the existing system may have to be modified. As a result, certain activities have to be repeated, which leads to an increase in the PET implementation costs. Section 7 focuses in greater detail on PET applications in existing systems.

Stor, Director of RINIS: 'During the development of RINIS, the PET costs mainly concerned the brainwork that went into the architecture. The costs of the different PET controls applied came to some 2 to 3% of the total development costs.'

Taal, Project manager at NTIS: 'The costs of the PET-specific parts for NTIS come to some 8 to 10% of the total costs, mainly because of the use of stringent authentication based on digital certificates that are protected with a pin code or with biometrically protected smart cards.'

The interviews with people in organisations where PET is used reveal that it is always possible to give a high-level estimate of the additional costs of PET. An accurate estimate is more problematic as the PET-related activities form a central part of the entire system development project from the design phase.

5.3 How do I arrive at a positive business case?

The knowledge required for preparing a business case can often be found within your organisation, albeit scattered, probably also with different visions being held of the costs and benefits. External information can often be useful too, for example from suppliers and government organisations using similar information systems and with longer experience with using PET. It may therefore be useful to organise a workshop around determining the business case. This is also desirable from the project management perspective because, in this way, a shared vision can be developed of the nature of the challenges, the precise objectives of the project, the anticipated costs and benefits and the positioning in relation to the organisation’s objectives.

To ensure the effectiveness of the workshop, in advance should be identified which questions need to be answered, what kind of information and documentation is available in the own organisation and which PET options need to be evaluated. This inventory should be distributed to the participants in order to prepare for the workshop. Aspects to be dealt with in the workshop include:

- the need for data protection controls for achieving the organisation’s policy objectives and targets;
- the target group of the public service developed;
- the potential benefits and the potential quantifying of the benefits;
- the possible PET options that can be applied and the corresponding one-off investment costs and structural costs (maintenance, management, licences) for each alternative;
- the application of existing resources;
- the impact on the processes and the working methods of the staff involved;
- the creation of support within the organisation for the application of PET;
- the presence and availability of the required knowledge and expertise;
- the agreement about the desirability of PET and the follow-up actions to be taken.

Based on the outcomes of the workshop, the final business case can then be prepared and the ‘go / no go’ decision taken concerning the application of PET in the information system involved.

Figure 18 shows an example of the costs and benefits of the implementation of a privacy management system (PMS).

Figure 18: Return on Investment from a Privacy Management System (PMS)

Suppose an organisation decides to implement a PMS. A sample business case could be substantiated as follows:

If PMS were not implemented, the minimum *annual* costs for an organisation employing 1,000 staff to comply with privacy policies are estimated as follows:	***Annual costs***
Salary costs Privacy Officer (100% time allocation)	€ 100,000
Management and secretarial salary costs	40,000
Costs privacy audit	30,000
Security costs with respect to privacy compliance (excluding generic information security required)	20,000
Report maintenance, regulations, settling registered people’s rights, information, image and other damage, etc.	20,000
TOTAL	**€ 210,000**

When using PMS:	***Development & implementation***	***Annual costs***
Acquisition of PMS	€ 150,000	
Consultancy for PMS implementation (60 days)	80,000	
Start-up costs after implementation	20,000	
PMS operational costs		30,000
Maintenance ± 15% of acquisition cost per annum		22,000
Costs privacy audit		10,000
Salary costs Privacy Officer (50% time allocation)	50,000	50,000
TOTAL	**€ 300,000**	**€ 112,000**

This table shows that the extra development costs for PET are already fully recovered after three years.

6 Organisational and legal aspects

PET concerns technology for the compliance with legislation; however, it relies upon legal and, in particular, organisational prerequisites for its proper application. This section focuses on:

- Management awareness and commitment (§ 6.1);
- PET as part of the management cycle (§ 6.2);
- The wicked triangle (§ 6.3);
- PET strategies (§ 6.4);
- The normative face of PET (§ 6.5);
- Verification and supervision (§ 6.6).

6.1 Management awareness and commitment

The PET application requires a effective implementation and an awareness-raising process with respect to data protection and PET itself. The system of controls and procedures implemented for the management, processing and security of personal data have to be tested against the objectives of implementing PET and, if required, be revised. The implementation of PET is not only a question of technology, but especially one of organisation and, as such, is also a primary responsibility of the organisation's management. Besides, it is important that the implementation of PET is not a separate component or a separate project, but that it is integrated as part of the system development and maintenance projects.

Director Kok (Trans Link Systems/public transport smart card): "We thought about the privacy requirements from the moment we invited tenders for the system design. We also chose the option of anonymous cards for the highest possible level of acceptance."

The implementation of PET is not something that happens overnight. An organisation needs time to get the awareness-raising process going. There is actually a difference between becoming aware of and thinking about data protection and the development and implementation of PET. It is advisable that the management responsible for the implementation of PET appoint one or more contact persons whose responsibilities include the coordination of the PET implementation and the evaluation thereof. Apart from the IT manager and the project manager, there is an important role for the Privacy Officer and the Security Officer.

6.2 PET as part of the management cycle

The implementation of PET puts demands on the processing of personal data and has consequences for the procedures and controls deployed by an organisation to properly manage and protect its data processing (reliable, efficient, effective, exclusive, accurate, continuously available and verifiable). An important precondition for the implementation of PET is an adequate system of general processing and IT controls, taking into account the specific safeguards required for the processing of personal data.

PET needs a prominent place in the management cycle if one wishes to implement and maintain a well-balanced policy for the processing of personal data, with PET forming a cornerstone of that policy.

Using the management cycle to achieve the business objectives and targets usually involves the following three phases: the organisation of the processes (including the policy-making), the processes themselves, and the evaluation and adjustment of the processes. It is important, in this context, to identify the administrative organisation insofar as it has not yet been done.

PET is part of the management cycle; therefore, a review should take place once a year to verify whether the PET solution(s) achieve the desired effect. This review can be performed as part of a privacy audit, which is carried out to see if the organisation has observed its privacy policies. The privacy audit is essential to examine whether PET achieves the desired effect and to provide feedback to the designers of PET-enabled systems.

The need for a risk analysis

The basic principle is to analyse and evaluate the processing of personal data from the privacy policy perspective, and then to set out how a PET implementation satisfies the requirements of the Data Protection Act. A risk analysis in advance is essential and useful for taking the correct controls, based on the relevant privacy threats and vulnerabilities. Several risk analysis methods can be used for this purpose, for example CRAMM, COBRA or SPRINT.

PET can only be successfully implemented after a thorough risk analysis that highlights the threats posed to the processing of personal data. The strengths and weaknesses of the data processing are also identified in this context. Specifically, this means that it must be clear, which personal data an organisation collects and processes, who has access to the data, who is responsible for the processing and whether the organisation has implemented sufficient controls to monitor compliance with the privacy policies.

Based on the privacy policies defined, the relevant risks, together with the strengths and weaknesses of the processing organisation and a cost-benefit analysis, lead to a well-considered choice for the required organisational and technical provisions. The management should then see to it that the chosen PET provisions are properly implemented.

Using a system of logging and monitoring (see § 4.8.1), the management should assess the extent to which the controls taken achieve the objectives of the prevailing privacy policies. The management should make clear in what way and with what frequency it wishes to receive information about the handling of personal data – based on the logging and monitoring. The results of the logging and monitoring activities form the basis for any corrective actions, adjustment of the technical controls and procedures or even amendment of the prevailing policies.

6.3 The wicked triangle

One particular problem in the development of information systems with sensitive data is the different perspectives the parties involved have on privacy. When sensitive information is processed, the Privacy Officer will specify requirements with respect to the protection of personal data. The Privacy Officer often has a legal background, and is less familiar with technological solutions. That is why the project needs IT staff that usually have little knowledge about legal issues in general, and privacy protection in particular.

The Privacy Officer, in fact, will be primarily skilled in ‘PET thinking’, and far less in PET as technology or IT solution. And exactly the opposite applies with respect to IT staff.

It therefore boils down to the fact that policy staff or process owners, for instance, have to fulfil a bridging role between ‘PET thinking’ and PET technology to enable both types of staff involved to make an effective and efficient contribution to the project. Without this bridging role, there can be a lot of misunderstandings and missed PET opportunities. Hopefully, this White Paper offers policy staff and process owners sufficient support to fulfil this bridging role for both disciplines with success.

6.4 PET strategies

Once the risk analysis has been carried out and the privacy threats identified, the management should make a choice between the different PET strategies to deploy PET for data protection. The following strategies can be chosen:

- The organisation focuses on preventing or reducing a person becoming identifiable.
- The organisation aims to prevent the unlawful processing of personal data.
- The organisation uses specific technologies that support data protection.

Of course, a combination of these strategies is also possible. The following paragraphs elaborate these three strategies in more detail. The PET strategies are allocated a place in the phased plan discussed in section 7.

6.4.1 The first PET strategy: the prevention of identification

It is important for the first strategy to determine whether there are identifiable data. A natural person can be identified directly or indirectly. A person is directly identifiable on the basis of a name and address, an identity number, a pseudo-identity that is widely known or a biometric characteristic (such as a fingerprint). Someone can be indirectly identified on the basis of other unique characteristics or attributes or a combination of both of these, from which sufficient information can be derived for identification.

With the aid of PET, the direct identification data in an information system can be anonymised. If the data have also been stripped of indirect identification features, no personal data are left whatsoever. In that case, the Personal Data Protection Act no longer applies as no personal data need to be protected.

6.4.2 The second PET strategy: to guarantee against unlawful processing of personal data

PET can be used to protect personal data against different forms of unlawful processing. It prevents personal data from being unnecessarily and unlawfully collected, registered, stored, distributed or consolidated internally or externally and linked (connected) to each other.

It is a basic privacy principle that no more data be collected and processed than strictly necessary for the agreed purpose.

Should an analysis show that fewer data can be used with PET, and that this principle can thus be satisfied, PET will actually have to be implemented. Moreover, PET contributes to observing the legitimacy of the purpose for which data are collected, because the technology can also block data if someone wants to use the data for a different purpose. PET is also ideally suited for use in the context of information security and not only vice versa.

6.4.3 The third PET strategy: the application of specific technologies to enhance privacy

Because the PET strategies discussed above cannot be applied in every situation, other technologies can be used to contribute to realising better privacy protection. For example, the use of privacy management systems provided by a range of IT suppliers. In these systems, the agreed privacy policy is consistently applied to all data processing.

An example of such a privacy rule could be:[Organisation] [may] [pass on] [client address] [by telephone] to [external contact] for [purpose] if [the client has given permission]

In the processing request, a specific name or condition is filled in every time between the square brackets on the basis of which the privacy management system decides whether the request is granted or not. The Privacy Officer fills in the possible conditions in advance; the privacy management systems provides practical support to specify these conditions.

Together, a sandwich of technologies can achieve privacy-safe data processing.

Privacy-enhancing technologies

Below are some examples of the use of technologies to boost privacy:

- Transparency is increased by the use of P3P (a technology for testing the privacy policies of websites).
- A statistical or linguistic analysis to verify the name or address inside an address files can improve the quality of the data.
- The rights of the individual (data subject) can be monitored more effectively through feedback and verification. These design principles ensure that information systems can at any moment provide feedback to an individual about the personal data the individual concerned has provided to the information system, with the option to consult, supplement, correct or erasure of personal data.
- The automatic deletion of data can also be used. Storage periods can be set in the software, and when that period expires, the specific personal data are automatically deleted.
- As far as manual processing and data transfer outside the EU are concerned, it is also possible to take technical controls to counteract actions in the meaning of the Data Protection Act. For example, by scanning IP addresses on the validity of the destination address. If the destination is outside the EU, the privacy management system blocks the dispatch. The system then asks permission from the management, and the dispatch is obviously logged if it goes ahead.

Figure 19: PET technologies

6.5 The normative face of PET

Section 13 of the Dutch Data Protection Act forms the legal basis for the use of PET. It stipulates that the person responsible for processing personal data take appropriate technical controls to protect personal data against loss and any form of unlawful processing. In addition, the controls must also prevent the unnecessary collection and unnecessary further processing of personal data. These controls are weighted on the basis of the following criteria:

- the status of the technology;
- the costs;
- the risks of both the processing and nature and scope of the data.

The requirement to apply PET is enforced in Section 11 of the Data Protection Act, which stipulates that no more, but also no less personal data may be collected and processed than are essential for the purpose. The responsible person is also responsible for taking the necessary controls to ensure that the data in question are collected and processed correctly and accurately as intended for the purpose.

The use of the slogan ‘**PET INSIDE**’ with information systems can have a positive effect on the awareness about PET.

PET is about the translation of ‘soft’ legal standards into ‘hard’ system specifications. This means that the installation of PET in systems is not only a technical exercise, but also a normative one. Before ‘PET INSIDE’[12] is incorporated in information systems, it must be clear what the requirements of the Data Protection Act for an information system are. Technologists and lawyers will have to translate the standards into technical system requirements.

6.6 Review and supervision

The Data Protection Authority (DPA) can call the responsible person or the third party processor to account for the organisation’s privacy policy, the protection and the processing of personal data and the way in which the system of controls taken is implemented and complied with. The DPA is authorised, by virtue of its office or at the request of an interested legal entity or natural person, to examine the way in which the Data Protection Act is complied with. The auditors of the DPA will then perform a privacy audit on the design, the implementation and the effective operations of the procedures and controls to guarantee the data protection in accordance with the legal requirements. The implementation of PET prevents the organisation from being confronted with unexpected and unpleasant surprises and creates the necessary public confidence in the authorities.

Apart from the audit by the DPA or other external parties, internal reviews and audits can also be carried out. This can be used to identify any further improvement of the prevailing privacy controls that may be desirable or even essential in order to comply with legal and internal requirements. Standard approaches and checklists are available for this purpose (see Appendix A.1).

[12] Phrase is borrowed from the ‘INTEL INSIDE’ advertising campaign.

7 PET plan

This section includes a phased plan for the implementation of PET. It focuses on both new and existing information systems, and deals with the following issues:

- PET as design choice (§ 7.1);
- PET in existing systems (§ 7.2);
- The phases (§ 7.3).

7.1 PET as design choice

The step-by-step PET plan only deals with aspects that are specific to PET and not with the general steps concerning the development and implementation of information systems. Before executing the phased plan, the organisation must recognise the importance of data protection. During discussions with project leaders involved in major projects where the application of PET was considered and/or implemented, the following rule was always prominent:

‘**Privacy by design**’

Data protection, including PET, should be part of the architecture of the information system, right from the start.

Before discussing the PET plan, § 7.2 first explains why it is important to include the implementation of PET as an integral part of the system development.

Case study 11: ‘Privacy by design’ in Canada: IT not only causes privacy problems, it also resolves them!

A survey conducted by the Alberta authorities revealed that some 57% of the content of their databanks consisted of directly or indirectly identifiable personal data. As a result, the design of a privacy structure within the Central Government of the Alberta Province in Canada was seen as a logical development. It would be an extension of the existing IT infrastructure and the Government of Alberta Enterprise Architecture (GAEA). The government of Alberta could use this privacy architecture to achieve its privacy policies with the aid of IT and ensure that the use of advance technologies comply with the legal privacy requirements.

The detailed requirements for the privacy architecture were agreed in October 2002 in a series of workshops organised across the authority with the relevant policy officials, the officials responsible for the IT infrastructure and representatives from the business community. These workshops resulted in a list of twelve requirements that were elaborated in detail in the GAEA Privacy Architecture Requirements policy document. Not only was an agreement reached about the shared privacy terminology, the essential user interfaces and the use of technology to enforce compliance, but also about an identity system based on meaningless but unique numbers (MBUNs)[13]. These numbers serve as reference to

[13] The MBUNs are not based on existing identification numbers.

deliberately fragmented and, as such, only partially accessible personal data domains. The concept of identification reference numbers is based on the use of identity protectors and layered identity domains. Following the specification of the requirements for the privacy architecture, a test model was developed, which was subsequently discussed and commented upon in the same working groups. Finally, the information obtained was used to set up the privacy management system, which received the HP Privacy Innovation Award in 2003.

7.2 PET in existing systems

PET is not a black box that one can buy and simply add to an existing system afterwards.

In practice, the implementation of PET in existing systems is usually a tricky exercise. If, for example, a change is made to recording data across different domains, the data model must be modified to meet the requirements of the domains and the new data flow. Both the application software and the database architecture of an existing information system have to be adapted accordingly. It may involve a substantial system modification, and therefore may become relatively costly. The user will actually notice very little as it mainly concerns technical modifications to the system.

Case study 12: Meerkanten Psychiatric Hospital

An in-depth privacy audit revealed that a psychiatric hospital complied with the prevailing privacy legislation on almost all fronts, except that the logical access security offered too many access and update opportunities. To guarantee proper protection of the information about people’s mental health, the hospital in question wanted to enforce access controls automatically for the care relationship between healthcare workers and patients. However, a hospital information system and a data model were already in use (X/Mcare system).

PET application

- separate identification data and medical information by using pseudo-identities. Thus only authorised people are able to combine certain data groups; other people can only access the identification data or the anonymous medical information. The medical information, in turn, is also registered in different domains to allow specific access for each type of healthcare worker. This PET application is known as the Privacy-Incorporated Database. As the data is anonymous, useful detailed information is available for scientific research;

- differentiated security for system access by staff. IT administrators do not have access to patients’ medical information. Access by external staff is controlled by stringent access controls with a mobile telephone and through encryption of the data traffic;

- registration of personal data provided to third parties for each patient concerned.

Benefits

The use of PET in the information system offers better possibilities to protect personal data. This not only complies with the Data Protection Act, but also with other healthcare-specific legislation with detailed privacy requirements. The users do not notice the existence of PET, unless they make an unauthorised attempt to access certain personal data. The PET application means the system can be connected to a future countrywide client tracking system; to this end, a trusted third party will have to be in charge of user authentication.

Conversely, anonymisation is easier to use in existing systems. In some cases, anonymisation tools can be added to the information system as 'accessory'. This can be done relatively easily with front-end systems, such as the organisation's website. The fact that anonymised data are now used does have consequences for the information system and the processes to be carried out. The processes will probably have to adapted since one no longer works with personal data. It is also quite possible to add a data warehouse to an existing information system for queries, selections, reports and other processes. This data warehouse will then periodically receive a selection of data from the production database, and thus contains anonymised data for statistical purposes.

It is expected that the introduction of a privacy management system that enforces privacy policies will require some investment, a significant part of which concerns the acquisition of supporting software. The software packages currently available do, however, contain functionalities to identify and reveal files and processes, which will make the implementation of privacy policies easier. There is limited practical experience in Europe yet, so little can be said about efforts in practice and the expected costs involved in existing information systems.

General PET controls can mostly be implemented effectively and efficiently after an information system has become operational. This then concerns, for example, the introduction of stricter authentication means, such as the use of smart cards, biometrical technology or digital certificates to gain access to a system.

The further sophistication of the authorisation structure based on roles or the restricted access to particular data can be added to a system at a later stage because these aspects mainly affect the system perimeter. However, the effort required strongly depends on the way in which the functionality is included in the existing information system.

Dynamic responsibilities and access control for a particular file ('rule-based'), as used in the healthcare sector and by the police and judiciary, can also be implemented as an element in an existing system with some effort.

PET controls that modify the system internally are possible, provided the control can be implemented in relative isolation. For instance, encrypting data in the database. This is technically possible without affecting the application system. Selective encryption, as referred to in the NTIS case study, requires more effort because it requires functional changes.

> Ter Avest, Financial Director and Supervisor at Meerkanten Hospital: ‘The success of the PET application is that you do not notice the PET technology in practice as a user until you attempt to access personal data that do not fall within your area of authority. As such, PET does exactly what we want it to do.’

The table in figure 20 illustrates whether it is possible to add the specific PET option to an information system afterwards.

	Before	**Afterwards**
General PET controls	Easily possible	Strongly depend on control and situation
Privacy management system	Possible	Possible
Anonymisation	Possible	Relatively easily
Separation of data	Easily possible	Tricky/expensive to do

Figure 20: Applicability of PET in existing systems

7.3 The phases

7.3.1 Justification & need analysis

The detailed elaboration of the privacy controls in the software and technical infrastructure is particularly prominent in the functional and technical design phases[14]. In practice, however, it is preceded by an essential phase in which the need and the intensity of the data protection have to be analysed.

First of all, it must be ascertained, which personal data are essential to provide the service. When determining the need for processing personal data, you should apply the principle ‘the less personal data we process, the better’. All things considered, data that are not collected cannot be misused, and less effort is required for the management and protection of the personal data. Numerous projects have revealed that, after a proper analysis, a significant amount of personal data did not have to be processed centrally or otherwise.

[14] Also known as: conceptual and system (architecture) design.

During this phase, you should bear in mind that several organisations and organisational units may be involved in the data processing. Every interested unit will want a say in determining, which personal data must be collected.

This phase produces a listing of personal data elements to be collected and the reasons for doing so.

Professor Boasson (University of Amsterdam): ‘This analysis often requires determination; there is still a lot of resistance against not collecting or storing certain personal data, with the argument that you may as well have the data in case it is useful in the future.’

7.3.2 Data analysis & classification: is PET useful?

Before an information system is actually designed, there is first a broad identification and specification of the essential features of the desired information system. The degree to which protection of personal data is required is one such feature.

Based on this step, the organisation can carry out an analysis to identify the threats and risks relevant for the data processing. The level of protection of the personal data for processing can be determined on the basis of the results from the risk analysis and data classification available in the organisation. The Data Protection Authority’s classification of risk categories can be used as a guideline.

Case study 13: Public transport smart card

It was decided in the Netherlands to replace the use of the national bus and tram card with the public transport smart card for several reasons:

- *users*: it increases user-friendliness and safety (no need to use cash);
- *transport companies*: it improves efficiency, it makes available reliable and up-to-date management information, it reduces the percentage of fare dodgers and increases staff safety.

This electronic payment system will be set up and managed by the Dutch organisation Trans Link Systems, and comprises the complete back-office settlement for its shareholders, the public transport companies. Where possible, the train, bus and metro stations will also be equipped with entrance gates for the public transport smart card. The smart card is suitable for all types of public transport and can be extended to associated (commercial) services in the future.

Name and address details of the public transport users are required for the financial settlement of the use of personalised cards – by means of a direct debit or charging the card in advance via a specially designed machine. In the other option, travelling with anonymous cards, the only possibility is to charge the card using such a special machine.

The system in the Netherlands is based on that in Hong Kong where so far more than nine million public transport smart cards have been issued, involving a few million transactions a day. The privacy legislation in Hong Kong is similar to that in the Netherlands since both are derived from the European Directive, and the system has proved successful in practice. Here, the same as in the Netherlands, one organisation is responsible for clearly formulating the privacy and security policies and for monitoring implementation and compliance.

PET application

- designing a layered architecture of the entire information system (smart card, entry gates, local processing, transport company processing and a central clearinghouse), with a distinction being made between the personal data that have to be registered at the different levels. On many levels, only the smart card and journey information are registered and no further personal data. Through the use of a data filter, only limited personal data are stored;
- encryption of sensitive personal data, such as journey and financial information. In addition, a closed network is used where possible;
- the use of anonymous smart cards that are charged manually with a cash value as travel credit;
- application of fraud and error detection functions on all the aforementioned levels. For tracing purposes, all a person's journey and transaction data from the different transport companies have to be combined;
- regular privacy audit in order to demonstrate that all the privacy requirements in the policy and the contract are continuously complied with. On the basis of the outcomes of the privacy audits, numerous improvements have been made to the security and privacy controls.

Benefits

Thanks to the use of PET, no single party can construct a complete profile of an individual person, and the system offers a basis for third parties to offer commercial services with sufficient guarantees for privacy (through a so-called opt-in scheme). All in all, the use of PET controls increases the confidence of public transport users, politicians, supervisory bodies, the media and other stakeholders. The lack of confidence in one of these groups would substantially lower the chance of success of such a complex project. Moreover, there have been no substantiated complaints about the protection of personal data in Hong Kong.

Now that a decision has been made about the desired level of data protection, it can be determined, partly on the basis of the privacy and security controls already taken, whether the application of PET is desired and how PET can contribute towards the data protection. A balance must be achieved between the organisational and procedural controls on the one hand and, the application of PET on the other. To this end, you can refer to the PET staircase in § 4.6 to determine which PET controls are required in view of the risk profile of the data processing, and to determine the level of ambition with respect to the application of PET.

Here a distinction can be made between:

- identity-rich: identifying personal data required;

- identity-low: identification required once, but a single characteristic suffices, such as age or profession; identity-free: no identity required) processes. With respect to identity-rich processes, general PET controls and privacy management systems in particular are applicable. For identity-low processes, the separation of data into domains, general PET controls and privacy management systems are well-suited. For identity-free processes, separation of data and anonymisation are the ideal PET options.

The business case must also be elaborated in this phase (see section 5). In addition, the objectives of the application of PET must be clearly defined and communicated within the project and the user organisation.

7.3.3 Functional design

In this phase, the system is described in functional terms and the process model is developed. The process model references to the data flows in the information system, including connections/exchanges with other organisations. The data model for every data flow in the process from compilation, registration, storage through to destruction must also be reproduced. The most important aspects involved in the creation of the process and data model for the processing of personal data are:

- the origin of the personal data (the use of authentic registers and connections with other databases, where applicable);
- the type of personal data (special information, if applicable);
- the type of processes (electronic decision-making, if applicable);
- users and user groups to whom the data is supplied (external recipients and recipients outside the EU, if applicable);
- the required level of self-determination by the individual, and duties to inform the public;
- the party in control of and responsible for the data (outsourcing, if applicable);
- storage period (mandatory destruction, if applicable);
- parties involved in the data processing (representatives and administrators, if applicable).

It will be clear that the chosen PET option will have a significant effect on these aspects. For instance, the separation of domains, one of the PET options, will have direct consequences for the data model and connections between the domains and any other information systems that derive information from the data in the relevant application. Anonymisation will influence both the data model (fewer data to register) and the processes. The application of a range of separate PET controls will also have to take place at this stage in order to avoid system modifications at a later stage. And the application of privacy management systems may well have little influence on the data model or the functional processes, the influence on the technical architecture of the information system will be greater (see next phase).

7.3.4 Technical design

In this phase, the functional design is further elaborated and detailed in a more technical sense. An important aspect is that the technical design of the PET option must be integrated in the complete technical design of the information system. The PET option is, after all, not a separate component that can be added; therefore, the technical design of PET cannot be separated from the technical architecture of the entire information system.

Appendix B contains a list of PET techniques to be used in the different PET options. A combination of PET options and techniques is also possible, as well as the use of individual PET controls, such as encryption or role-based access controls.

7.3.5 Development

It should be decided during the development phase whether the organisation will design the selected PET options and the corresponding techniques itself, or whether a standard software package will be bought. There is already a fair amount of standard solutions on the market for anonymisation and for logging and monitoring. If the ‘separation of data’ option is used and different domains are created, it is likely that quite a bit of component customisation will have to be performed.

Some standard software is available on the market for applying privacy management systems. Account should be taken, however, of the effort required to translate privacy policies into specific privacy rules that, in turn, have to be programmed into the chosen privacy management system. Besides the list of PET options and techniques, Appendix B also lists the techniques that are already available and those that have to be developed by the organisation.

7.3.6 Testing

Once the information system has been developed, an assessment must be made to ascertain whether the system operates properly and whether the users accept the new system. The tests should also include the PET functionality and its user-friendliness. In view of the maturity of PET, it is advisable to start off with a small-scale pilot project. Based on the results of the pilot project, the PET-proof information system can then be adapted, if applicable, and rolled out in the entire organisation. During the tests, account should also be taken of the degree that the system lends itself to scaling. For instance, a particular implementation project revealed that the system did not function entirely correctly in a large-scale implementation, whereas it did in an environment with small-scale use.

When the chosen solution is one with a privacy management system, the test will certainly have to focus attention on the privacy rules installed in this system. Little experience has been gained with using the particular syntax (often resembling XML), and the Privacy Officer will most probably have prepared the syntax, also with little experience with it.

7.3.7 Implementation

In this phase, the information system, together with the PET option, will be implemented and the organisation will start using the PET-proof system. Over and above the normal implementation activities, it is essential to ascertain what needs to be done for PET to work. For example, in the case of data being separated, authentication tools have to be issued for users to use the identity protector. The issuance and, in particular, the granting of authentication tools must not be underestimated. It forms the basis for the proper functioning of the PET option. Of course, communication regarding the new system and the implementation of PET play an important part during the implementation process – at least when PET has any effect on the usability of the system. Part of the communication includes the training of the users and the administrators in the use of PET.

When preparing for the implementation, it is advisable to find out whether the chosen PET tools, for example a smart card, can be provided to all users within the agreed timeframe.

7.3.8 Management & maintenance

In addition to the standard management and maintenance tasks involved in an information system, and thus also in the PET option, there are also PET-specific management and maintenance tasks. For example, authentication tools and access controls also have to be managed. People may lose the smart card or token, forget the relevant PIN code, change position, etc. A management process should therefore be set up around the authentication tool and the authorisation of people.

7.3.9 Evaluation

The project must be evaluated, to which end an evaluation plan and evaluation criteria can be drawn up. The effectiveness of the PET controls can be assessed on the basis of this post-implementation evaluation, among other things. Where needed, adjustments can be made to the information system and the PET option on the basis of this evaluation.

A privacy audit can provide the necessary support if it also addresses technical aspects and the PET options. An organisation can also decide to have its information system or its business process handling personal data certified in the context of the Data Protection Act.

Case study 14: Online medical history file

Together with the Dutch Applied Scientific Research organisation (TNO) and a trusted third party (Diginotar), the Dutch Council for Chronically Ill and Disabled People (CG Council) developed an online medical history file. This so-called ‘digital experience file’ enables all members of 140 organisations affiliated to the CR Council to keep their medical information up-to-date.

PET application

- independent issuance of authentication tool by the trusted third party. It offers the choice of authentication by means of user-ID and password, mobile telephone or a bankcard, depending on the requirements of the Internet application. An ownership feature (such as mobile telephone or bankcard) is the minimum requirement for access to the online medical history file.

- use of pseudo-identities for anonymous access to the digital history file. The same trusted third party is responsible for managing the pseudo-identities. The CG Council and TNO are unable to make a connection between the real identity and the pseudo-identity. No identification data are required for many service applications, such and healthcare and prevention sites of insurance companies;

- certification of the reliability of the third party and the Internet applications that process the medical information. Certification is achieved with the aid of the QMIC® system;

- users indicate which medically-related historical data they wish to make available to third parties and in which research projects they wish to take part.

Benefits

Chronically ill and disabled people can use this system to keep their own medical history up-to-date in a safe and flexible way. They are also ensured that their medical history and their personal data will be properly looked after by the research organisation and trusted third party respectively. Moreover, their personal medical history file is connected exclusively to QMIC®-certified information services.

Of course, the users' experiences are also relevant and should form part of the evaluation. It is also vital to use the evaluation to identify learning opportunities for the development project, for example, in the field of efficiency, project approach and the integration of PET therein. These learning opportunities are useful for the organisation itself, but can also support other organisations wishing to implement PET. During the evaluation, the costs incurred and benefits realised (the added value of PET) can also be compared to the prepared budget and business case.

7.3.10 Product categories

Figure 21 includes a table showing which product categories with specific PET elements should be prepared in which phase.

Project phase	**Project categories with PET-specific elements**
Justification & need analysis	■ Summary of which data are processed and why.
Data analysis & classification	■ Data classification; ■ Risk analysis concerning data protection; ■ Report of the definition study, including the business case for PET.
Functional design	■ System design in which PET is integrated; ■ Data and process model.
Technical design	■ Detailed design of the system architecture.
Development	■ Decision regarding the purchase of a preferred solution (which package to buy) or custom development.
Testing	■ Test plan for specific PET aspects. This plan must form part of standard test plan.
Implementation	■ Communication and training plan; ■ Rollout plan for authentication tools if applicable.
Management & maintenance	■ Manual for the management and maintenance of specific PET components. Incorporate manual and activities in standard manual and activities.
Evaluation	■ Evaluation and/or auditor's report.

Figure 21: PET-specific product categories to be implemented in each phase

8 Actions

You intend to seriously evaluate the possibilities for the use of PET in the information systems falling under your responsibility. What can you do in the short term to ensure the successful application of PET in your organisation? The summary below briefly presents the success factors based on our experience in these projects and suggestions offered by the people interviewed from their practical experiences.

- Identify the most important running or forthcoming projects concerning information systems processing personal data.
- Organise a PET awareness-raising session for the responsible process owners, policy staff, programme and project leaders and privacy and security officers, and promptly clear any misunderstandings concerning data protection and the required PET controls. Supplement this with awareness-raising materials for all the stakeholders involved, consisting of this White Paper, a flyer and information about best practices.
- Make sure that 'PET thinking' is embedded in the organisation, with PET being a serious option for all new and existing information systems that process personal data.
- Argue from the perspective of the organisation strategy and the management model when it comes to data protection and the application of PET.
- Strike a good balance between the anonymity of the person concerned on the one hand and, on the other, knowing the client, enabling tracking and combating fraud. In some instances, there is no need to know someone's identity, simply the fact that it concerns one unique person, and sometimes there is a need to know the client. Using a number as protection against using the name is an option in this respect. To find the right balance, the processes can be divided into identity-rich, identity-low and identity-free processes.
- Determine and properly substantiate in advance the minimum set of data required in a specific situation, and what additional information may be required.
- Make a proper distinction between the demands and wishes concerning data protection and the corresponding PET controls.
- At the same time, improve the quality of the personal data (the so-called 11-test on tax and social security numbers is a good example). Reliable data form a solid basis for the acceptance of authentic registers and data protecting controls and the countering of duplicate administration.
- To achieve optimum effectiveness of the PET controls, it is essential to refine the organisation's authorisation structure step-by-step. For example, defining the functions and the roles and introducing role-based access controls.
- Use the results of privacy audits and the pattern of any privacy-related complaints to substantiate the need for PET. Perform a regular privacy audit or evaluation to further improve the PET controls.
- In the case of inter-organisational connections and data exchange, discuss the need and desirability of a possible PET application with partners in the chain. Also agree upon clear guidelines with all the parties involved to strengthen the effectiveness of the PET application.
- Maintain the flexibility of other organisations with which data are exchanged. Choose a basic central model for retaining local autonomy and responsibilities. There should be no or only very limited central interference with the chosen method of data exchange and very restricted or no central access into the message content.

- Select a suitable information system for a pilot project involving application of PET, and choose a phased approach that is not too ambitious or too rigid in interpreting privacy right from the start.
- Pay particular attention to including the transparency principle right from the start in the design of the PET application.
- Position PET solutions as an infrastructural ‘utility’ that benefits numerous projects and not merely a drain on the budget of the pilot project. After the pilot project, incorporate the PET application method in the system development method and incorporate PET components in the information and system architecture.
- Ensure that the users experience little hindrance and mainly benefits from the PET application.
- Concentrate on and explore possible financial support from subsidy schemes.

Finally:

To summarise

PET is more than simply a means of protecting personal data:

- **PET is attractive!**
  - PET enhances the quality of information.
  - The dependence on proper compliance of processes and procedures is reduced by the automatic enforcement of privacy regulations.
  - The application of PET can offer the public better insight into and control over their personal data.

- **PET is imperative!**
  - With PET, it is easier to comply with the Data Protection Act.
  - PET provides the conditions for public confidence.
  - PET enables working with sensitive personal data.

- **PET is possible!**
  - PET has been successfully implemented on numerous occasions, which is evident in this White Paper
  - PET has only a limited effect on the costs of developing a new information system, since the technologies are available and it mainly concerns the application. The ‘cost’ mainly involves thinking and designing.
  - Implementing PET in your information architecture offers the basis for efficiently applying PET in different information systems efficiently.

Figure 22: Reasons for using PET

A Bibliography

The terms added in square brackets refer to a number of references concern the PET techniques mentioned in Appendix B.

A.1 PET in general

- Borking, J.J., Raab, C., Laws, PETS and other technologies for privacy protection, *Journal of Information, Law and Technology*, no. 1, February 2001.
- Dutch Data Protection Authority, *Studies and Investigations 11: Privacy Enhancing Technologies: the path to anonymity*, September 1998. *[Blind elektronic signatures, Privacy Incorporated Database, Biometrics]*

A.2 PET case studies

- Campbell, A., *Privacy architecture*, Government of Alberta, November 2003. *[Privacy Incorporated Database, EPAL, Privacy policy management, Cryptography-based IDs]*
- IBM Global Services, *Privacy architecture overview of the government of Alberta*, May 2003. *[Privacy Incorporated Database, EPAL, Privacy policy management]*

A.3 PET in depth

- Borking, J.J., *The status of privacy enhancing technologies, Certification and security in E-services: From e-government to e-business*, ISBN 1-4020-7493-X, Kluwer Acadamic Publishers group, 2003. *[P3P, PISA]*
- Borking, J.J., Kenny, S., The value of privacy engineering, *Journal of Information, Law and Technology*, no. 1, March 2003.
- Borking, J.J., Privacy rules for intelligent software agents, *Tilt*, no. 15, 2003. *[PISA]*
- Escudero-Pascual, A., To be or not to be in the next generation Internet, *Tilt*, no. 15, 2003. *[Cryptography-based IDs]*
- Karjoth, G., Schunter, M., Waidner, M., Privacy-enabled services for enterprises, *Tilt*, no. 15, 2003. *[EPAL]*
- Kenny, S., Korba, L., Applying digital rights management systems to privacy rights management, *Computers & Security*, no. 7, 2002. *[Privacy rights management]*
- PISA consortium, Handbook of Privacy and Privacy-Enhancing Technologies: the case of Intelligent Software Agents, 2003. *[PISA]*

A.4 Websites

- www.cbpweb.nl/en
- www.pet-pisa.nl *[PISA]*
- www.w3.org/P3P/ *[P3P]*
- www.cdt.org/privacy/pet/p3pprivacy.shtml *[P3P]*

B PET technologies

This appendix includes a summary of possible technologies that can be used to apply the PET options dealt with in this White Paper. A distinction has been made between standard solutions, custom-built solutions and future solutions. A further explanation and information about the technologies described in the table can be found in literature listed in Appendix A. The technologies discussed in the relevant document/website are also listed at a number of articles in Appendix A.

	Available	**Custom-made**	**The future**
General	■ Encryption (storage & communication) ■ Logical access controls (authentication and authorisation)	■ Biometrics ■ Quality-Enhancing Technologies	■ Cryptography-based IDs ■ Government access facility (e.g. portals)
Separation of data	■ Profile management	■ Privacy incorporated database ■ Blind electronic signature	■ Personal data safe
Anonymisation	■ MIX routers ■ Onion routers ■ Cookie management tools ■ File management tools	■ Smart cards ■ Biometrics	
Privacy management systems	■ P3P (Platform for Privacy Preference Project)	■ Privacy Rights Management (based on Digital Rights Management) ■ Automatic data destruction (retention management)	■ PISA (Privacy-Incorporated Software Agent) ■ Privacy ontologies ■ EPAL (Enterprise Privacy Authorisation Language) ■ Privacy policy management software

Figure 23: PET technologies

C List of definitions

Authentication tool

An authentication tool is a means used to confirm that a person in fact is who he/she claims to be. This could, for example, be a digital certificate, but also a token or username/password combination is a form of authentication.

Citizen Service Number

The Citizen Service Number is a user number that the Dutch central government will issue to all citizens. With the implementation of the citizen service number, persons can utilize a single number for all contacts with the authorities. Authorities, in turn, can perform their tasks more effectively with the use of the citizen service number because it enables faster, more efficient and more reliable data exchange. The use of personal numbers serves three purposes: it improves the service to clients, combats identity fraud and increases the government's transparency with the aim of improving privacy.

Special categories of personal data

Pursuant to the Dutch Personal Data Protection Act, it is prohibited to process personal data concerning someone's religion or philosophy of life, race, political persuasion, health, sexual life, as well as personal data concerning membership of a professional association, criminal record and personal details about unlawful or objectionable behaviour with respect to a sanction imposed because of that behaviour. This prohibition can only be lifted if certain stringent conditions are satisfied.

Digital signature

A signature consisting of electronic data that are attached to or logically associated with other electronic data and that are used as means of authentication. An electronic signature based on a qualified certificate satisfies the legal requirements in the same manner as a handwritten signature. The national digital signature legislation is based on the European Directive 1999/93/EC, further elaborated in the technical standard ETSI 101 456.

EPAL

Enterprise Privacy Authorisation Language (developed by IBM and ZeroKnowledge) is a language for describing the relationship between objects (see *privacy ontology*) for use in privacy management systems in order to automatically realise the processing of personal data within the legal frameworks.

Identity protector

An element in an information system that protects the identity of the user, the citizen and the consumer, and that controls the exchange of the identity between the various other elements in the information system. The identity protector converts the identity of the individual concerned into one or more pseudo-identities. The use of an identity protector creates a minimum of two types of domains; these are domains in which the identity is known or accessible and domains in which this is not the case (see also PID).

Personal fact

Every fact concerning an identified or identifiable natural person (also referred to as 'personally identifiable information').

Personal Data Protection Act

The Dutch Data Protection Act took effect on 1 September 2001, and it represents the implementation of European Directive for the protection of personal data (95/46/EC) and replaces the old Personal Data Registration Protection Act. The Directive took effect on 24 October 1998.

PET

Privacy Enhancing Technologies (PET) is a collection of information and communication technologies that strengthens the protection of individuals' private life in an information system by preventing unnecessary or unlawful processing of personal data or by offering tools and controls to enhance the individual's control over his/her personal data (Source: TNO).

PID

The data in a Privacy Incorporated Database are separated in an identity domain and a pseudo-identity domain. The so-called identity protector creates the connection between the different domains. If a person has no access to the identity protector, he/she cannot make the link between the data in the different domains (see also *Identity protector*).

PISA

The Privacy Incorporated Software Agent project is a research project subsidised by the EU in which software agents (digital agents) are built to protect the privacy of users of personal digital assistants on the internet. See further: www.pet-pisa.nl.

PKI

A Public Key Infrastructure uses public key cryptography to make a reliable connection between the identity and other attributes of the holder of the private key and certificate. A PKI uses digital certificates issued by a Certification Service Provider (CSP).

Privacy

An internationally recognised basic human right: Respect for and protection of privacy, including the lawful processing of personal data, and, in the Netherlands, laid down in the Constitution, the Data Protection Act and numerous other laws.

Privacy ontology

Ontology is a formal machine language understood by an information system and that describes certain knowledge elements and their mutual relationships in a particular knowledge field. Privacy ontology describes the knowledge about the data protection knowledge domain in a standard, unambiguous manner with the aim of converting privacy legislation into a language that is understood by an information system so that the system in question automatically applies the prevailing privacy legislation to the processing of personal data, thus preventing unlawful processing.

Privacy Rights Management

Privacy Rights Management concerns the protection of personal data by means of a method based on digital technology to protect copyrights registered on data carriers (Digital Right Management). The aim is to provide personal data with an inextricable digital label containing the privacy preferences.

P3P

The Privacy Preferences Protocol is a tool that enables easy communication about the privacy preferences of internet users in standardised form that can be read by the information system.

Quality Enhancing Technologies

Quality-Enhancing Technologies is a collective name given to technologies that improve the quality of data processing and data itself. These technologies form a subset of PET.

Smart card

A digital data carrier fitted with a microprocessor with the capacity of a small computer, which can be used for numerous purposes, including a debit card, identification and authentication (see *authentication tool*), access control, reference index for medical information, loyalty card, etc.

TTP

A Trusted Third Party that delivers reliable and confidential services, such as reliable hosting services or the issuing of digital certificates (at present, the party issuing digital certificates is indicated with the term CSP).

W3C

The World Wide Web Consortium is a consortium concerned with the development of interoperable technologies (standards, software and tools) for the internet. Among other things, W3C developed and improved P3P (see *P3P*). The JRC (Joint Research Centre of the EU situated in Ispra, Italy) developed a version of P3P in accordance with the EU Directive.

D Case Studies included with PET application