IS/2007/ENPAP/JH/01
"Strengthening Data Protection in Israel"

Activity 1.1:
Analysis of the Legal Framework on Data Protection

A guide to data protection in Israel.

By Ian Bourne – Head of Data Protection Projects, Information Commissioner's Office, UK

January 2010

The Israeli Law, Information and Technology Authority (ILITA)
The Government Campus 9th floor, 125 Begin Road – Tel Aviv - Israel

Contents:

About this guide.

This guide provides a brief, accessible introduction to data protection law in Israel. It should also be of use to any person or organisation that needs develop a general understanding of Israel's approach to data protection, perhaps because they need to do business in the country. It gives a brief description of Israel's Data Protection Authority, the Database Registrar within the Israeli Law Information and Technology Authority (ILITA). It does not provide an exhaustive analysis of Israel's law or of its legal system.

1. The Israeli legal system

In order to understand how data protection law works in Israel, it's necessary to understand the Israeli legal system. The Israeli legal system is a unique hybrid. It has continental, North American and common-law influences. These come together to give practical effect to Israeli privacy law.

As a common law country, Israel's laws are interpreted and developed through the specific decisions of the courts. Its judiciary enjoys wide judicial power and discretion in making case law, something that is guaranteed in Israel's 'Basic' laws – these are described later in this paper. It is important to understand that the principle of precedent in Israeli law means that a decision in of a higher court will bind a lower court, and the Supreme Court is not bound by its own decisions.

A growing body of court rulings is defining the character of the Israeli data protection regime. It is clarifying how Israeli data protection law applies in real-life situations, explaining how the balance between privacy protection and the collection and use of personal information should be struck. However, the differences between Israel's essentially common-law system and a civil law system (as in most of Europe) should not be overestimated. Both systems start off with bare legal texts. These are given meaning by regulatory actions by Data Protection Authorities and by tribunal and court rulings. These elaborate the principles and definitions that constitute applicable law.

The Israeli legal system is a hierarchy consisting of several tiers. At the top are the 'Basic laws', which enshrine constitutional values and rights. This means that the power of the legislative, and the executive branch, to interfere with these rights is limited. According to Israeli constitutional jurisprudence, any court can declare a law conflicting with the Basic laws to be "unconstitutional" and therefore null.

Below the Basic laws are regular laws, and below these various acts of the executive branch (Ministers), which are administrative regulations. As in other legal systems, the lower tiers are subordinate to the higher ones, and the overarching influence of Israel's Supreme Court and Basic laws should not be underestimated. Israel's Supreme Court has wide discretion and applies an active interpretive approach, which shapes and regulates administrative discretion. Where a right protected by the Basic laws is interfered with, the relevant Basic law will be the touchstone against which the provision in question is tested

2. Israel's 'Basic laws'

Like the UK, Israel does not have a written constitution. However, its system of Basic laws now has a de-facto constitutional status. This means that even laws passed in the Knesset must comply with the overarching values enshrined in these laws.

The Basic laws are similar to those found in Canadian constitutional legislation. They set out the overarching standards that Israeli institutions - legislative, executive and judicial - must adhere to. From a privacy perspective, section 7 in the Basic Law: Human Dignity and Liberty is most relevant. This states that:

(a) All persons have the right to privacy and to intimacy;
(b) There shall be no entry into the private domain of a person without that person's consent;
(c) No search shall be conducted in the private domain or on the body of a person , nor in the body or effects of a person;
(d) There shall be no violation of the secrecy of the communications, writings, or records of a person.

This broad and absolute right is qualified by a "limitation clause" in section 8. The limitation clause requires that any act, including legislation, which limits the rights set out in the Basic Law, including the protected right to privacy, must itself:

1. befit the values of the state of Israel
2. be for a proper purpose, and
3. not violate the right to a greater extent than is required.

These protections have a similar effect to the tests of legitimacy of purpose and of proportionality which are key concepts in European human rights and Data Protection law. For example, the third test is in effect very similar to the continental "proportionality" test.

Where there is a contradiction between laws, the relevant Basic law will prevail. In this respect the Basic laws have a similar effect to the human rights principles that underpin much European law. For example, the relationship between section 7 of the 1992 Basic Law: Human Dignity and Liberty - which provides for a general right to privacy - and the Protection of Privacy Act ("PPA") mirrors that between Article 8 of the European Convention on Human Rights and European national data protection laws. To sum up, the Basic law provides a clear constitutional direction to the Israeli administration and all levels of its judiciary to respect the individual's right to privacy, and inspires jurisprudence in this field.

3. The Supreme Court

Sitting as a High Court of Justice, Israel's Supreme Court is a powerful body which is unusually accessible to the general public, relative to equivalent courts in other jurisdictions. This can give effective redress to individuals. A development in case law in recent decades has enabled petitions in the public interest, without the need to show an individual particular grievance - somewhat similar to Freedom of Information principles. This can give concerned individuals, and pressure groups, direct access to the country's highest court in cases where they believe that a law or policy does not serve the general public good. This right is particularly valuable to Israel's many public advocacy groups, who use this tool extensively to influence policy-making. The right is used by politicians, journalists, law students, NGO's and civil society groups of various kinds, such as the Association for Civil Rights, as well as by members of the public.

The Supreme Court is also unusual in that it has traditionally been willing to rule on issues which, in other jurisdictions, would be considered to be the policy prerogative of the government or legislature. It sees one of its primary roles as being to ensure that the government complies with the state's own overarching rules. Whilst this can undoubtedly cause tension, for example when public appointments are challenged, it does mean that individuals have an effective source of redress should they believe that a law or governmental policy objective is not in the public interest. This reflects a long tradition of the Supreme Court hearing individuals' petitions against the conduct of the state.

The Supreme Court can strike down laws or regulations when they conflict with Basic law and fail the limitation clause tests, or it can require that regulations be put in place to provide a particular safeguard. For example, the Supreme Court has used the tests in the limitation clause to require the government to introduce safeguards in the case of data transfer from the Ministry of the Interior to private sector financial bodies. Although the transfers were authorised by statute, the court held that the legal basis for the transfer lacked specificity, had a disproportionate effect on personal privacy and therefore failed the triple test of the limitation clause. The court ruled that certain 'classical' data protection safeguards had to be put in place before the transfer could resume, for example the recipients and use of the data had to be specified in greater detail and information security had to be improved. This reflects the ability of the Israeli courts to translate the broad principles of the Basic law into practical data protection compliance measures.

4. Privacy Protection Act 1981

The Privacy Protection Act (PPA) forms the main element of Israeli data protection law. It has two main elements. Chapter One of the PPA deals with general privacy protection, including the "classic" privacy torts. It applies to a person's privacy, whether or not it involves the collection of data on a database. Chapter Two deals specifically with databases, and is much closer to 'informational' data protection law than Chapter One. However, Israeli jurisprudence has extended Chapter One's general privacy protections to the realm of data protection, thereby creating significant overlap between the two chapters. This means that data subjects' rights are protected not only by Chapter Two, but also by Chapter One, which sets out, for example, the principles of purpose limitation and informed consent.

It is important to appreciate that Chapter One of the PPA is not intended to be a data protection law. It deals with a much wider concept of privacy and therefore deviates significantly from the European Data Protection Directive, which it predates by some fourteen years.

The first clause of Chapter 1 of the PPA prohibits the infringement of privacy, unless the individual consents to this. It then goes on to define infringement of privacy as being any one of eleven specific wrongs. These include:

- spying or trailing a person in a manner likely to harass him
- photographing a person whilst he is in the private domain
- publishing a person's photograph in circumstances in which the publication is likely to humiliate him or bring him into contempt
- using a person's name, title, picture or voice for profit
- infringing a duty of secrecy laid down by law in respect of a person's private affairs
- infringing a duty of secrecy laid down by express or implicit agreement in respect of a person's private affairs
- using or passing on information about a person's private affairs for a purpose other than that for which it was given

It is clear, therefore, that this part of the PPA is intended to prevent specific privacy infringements, rather than to regulate the processing of personal data in general - as is the case in 'classical' data protection law.

The list of privacy infringements in the PPA itself is not absolutely comprehensive, although many of the infringements are drafted so widely as to catch much privacy-invasive activity. The PPA's 'infringements' are perhaps best interpreted illustratively rather than comprehensively –

they indicate the *sorts* of wrongs that the law is intended to prevent, and the Israeli courts have adopted this purposive approach.

Some of the terms used in the PPA's list of infringements are defined in the PPA, for example 'use' [of information]. However, it is clear that many of the infringements' key concepts, notably 'a person's private affairs', are open to a wide range of possible interpretations. This can clearly cause practical uncertainty and can expose difficult issues for the regulator and the courts. For example, to what extent can an individual employee expect to have his or her *private affairs* respected in the work-place? All jurisdictions have been faced with such questions in the context of their own data protection laws. However, there is no doubt that given the way this part of the PPA is drafted, a particular responsibility is placed on the courts to make sure that, in a particular case, the right balance is struck between personal privacy and the legitimate collection and use of personal information.

Chapter one of the PPA applies to the privacy-infringing activity itself, whether or not it results in the collection of personal information. In the European data protection model, spying or trailing a person would not fall within the scope of data protection law unless it involves the processing of personal data – for example collecting CCTV footage or compiling a log of a person's movements. In the PPA, the surveillance activity itself is regulated. This reflects the fact that Chapter one of the PPA is a general privacy law rather than a data protection law. It is true to say that in Israel, 'informational' data protection is a subset of a much wider concept of personal privacy, and the difference between Chapter One and Chapter Two of the PPA reflects this.

The Chapter 2 of the PPA is specifically concerned with information kept on a database. It therefore corresponds more closely in scope with the 'informational' data protection law found in Europe and elsewhere.

This part of the PPA also contains definitions of 'information' and 'sensitive information'. It is clear that this part of the Israeli law works differently to the European Directive. There is no definition of personal data based on the possibility, or likelihood, of an individual being identified. Instead, the Israeli law specifies that 'information' means 'data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs' of a person. Whilst this is a fairly comprehensive definition, on the face of it, the Israeli law is narrower in scope than the European one. However, the Israeli courts have taken a very wide view of personal information. For example, in *Database Registrar v. Ventura*, the Supreme Court held that the term "information" includes details such as a person's address and telephone number, bank account number and national ID number. These details are not specifically included in the definition of "information" in Section 7 of the PPA. However, the Supreme Court held that the capacity of computerised databases to store, match and transfer large volumes of information, which could be used to compile blacklists against the interests of data

subjects, requires a broad interpretation of the term "information". In effect, this narrowed the gap between PPA and continental definitions of personal data. In fact, *Ventura* was a data protection case, concerning with the registration of a credit referencing database. Its reasoning has since been applied in a series of data protection cases. In another case, for example, in one case concerning vehicle owners, the court held that:

"the term 'information' apparently refers only to data concerning an individual person (Section 7 of the PPA). Yet I do not believe it should be interpreted so narrowly as to exclude data such as those concerning automobile license plates discussed herein. The term 'information' must be interpreted in line with the legislative intent of the PPA. It should include data that can be derived from a database which is not indexed according to individual names. In other words… if financial data concerning an individual can be derived from a database that is not indexed on a personal basis, it should be regarded as 'information' under Section 7 of the PPA".

The Israeli courts have also held that IP addresses are subject to the PPA, indicating that they are willing to construe personal information widely.

The PPA sets out various registration, purpose-limitation, transparency and security requirements, as well as individual rights of access and rectification. These requirements are linked to the size and nature of the information stored, on how the information was collected (directly or indirectly) and on whether the database is a public sector one or is used for direct marketing. It is clear that the intention of the law is to target databases that contain information whose processing has the potential to cause a privacy infringement – eg public sector databases or ones holding employees' financial details. This reflects the 'risk' approach that is implicit in Israeli privacy law. However, whether or not a database is required to be registered, other legal requirements – eg security – still apply to it.

The 'databases' chapter of the PPA also gives the individual the right to inspect personal information about him or her kept in a database, and to have any information that is inaccurate, incomplete, or out of date amended. However, on the face of the legislation, this right falls short of the subject access right that is a key feature of European and other data protection laws. However, there is now jurisprudence indicating that the right of inspection includes the right of the individual to obtain a copy of any data related to him held by a controller.

Part 1 of Chapter 2 of the PPA also introduces security obligations for all databases, including a professional duty of secrecy for those having access to a database and the appointment of security supervisors for possessors of multiple databases, public bodies and certain financial institutions. This part of the PPA, with compliance requirements varying according to the number of databases held, is clearly showing its age. It was obviously drafted at a time when databases were separate entities, with little or no interconnection.

Part 2 of Chapter 2 deals specifically with direct marketing. The rights relating to direct mailing, most obviously the right to prevent it, only apply where the information used is held on a database and where the mailing is targeted at a person or persons with a particular characteristic. Israeli telecommunications law also includes specific rules banning "spam" and automatic direct calling. In practice, the Ministry of Communications, rather than ILITA, deals with 'automatic communications' such as spam. 'Traditional' direct marketing *is* regulated by ILITA.

The PPA's direct marketing provisions require those operating a database to keep a record of the sources and disclosures of the information. This is an example of statutory foresight, given the age of the legislation, which has become more relevant in the context of modern list brokerage and commercial information sharing.

Chapter 3 of the PPA sets out the defences, burden of proof and mitigation in relation to criminal and civil proceedings for infringement of privacy.

Chapter 4 also reflects statutory foresight in recognising that the disclosure or sharing of information by public bodies is a particular privacy risk. This chapter starts off by prohibiting the 'imparting' of information by a public body unless there is lawful authority or individual consent for this. It then goes on to specify the conditions that must be satisfied for the imparting of information to be permitted; imparting the information must take place within the powers or duties of the body concerned, it must also be required for implementing an enactment, or be required for carrying out the receiving or disclosing body's functions, or for exercising their powers. Information can also be imparted to a public body with the lawful authority to demand it. Information can also be provided from a public body to a government body or other state institution, provided this is required for implementing an enactment or for exercising the public body's powers or carrying out its functions. (The concept of 'requirement' in this part of the PPA equates to the European concept of 'necessity'.)

This part of the PPA ends by imposing various purpose limitation, confidentiality, information assurance and registration requirements on public bodies that impart information.

Chapter 5 of the PPA, its final chapter, starts off by stating that the PPA applies to the state, and that enforcement can be taken against state bodies. It then sets out various provisions relating to proceedings, the powers of the courts, the admissibility of evidence, offences and damages. It also contains provisions relating to the publication of privacy-infringing material in newspapers, and sets out who is liable for this.

It is worth noting that the penalties available to the courts under the PPA for an infringement of privacy, or an associated offence, are considerably more severe than those available in most other

jurisdictions. For example, a person who wilfully infringes the privacy of another, for example by publishing intimate details of his or her life, is liable to a period of 5 years' imprisonment.

5. Further development of the Personal Privacy Act

The PPA has been amended nine times since its adoption. A recent amendment clarified the standard of consent needed to legitimise the collection or use of personal information; it must be 'informed'. Another amendment has strengthened the individual's right to claim compensation for a privacy violation, even where there is no proof of damage. In 2001 regulations relating to the overseas transfer of information held on an Israeli database were introduced. These broadly replicate the 'adequacy of protection' provisions of the European Data Protection Directive. However, the PPA is currently in the midst of a much more comprehensive and radical overhaul.

In 2005 the Ministry of Justice set up a committee to review the fitness for purpose of Chapter 2 of the PPA – the part that deals with databases and that most closely resembles mainstream data protection law. The committee – generally known as the Schoffman Committee, after the Deputy Attorney General who chaired it - consisted of various privacy specialists, academics, government officials and lawyers. The brief of the Committee was not to replicate European or other data protection law. However, the Committee was clearly mindful of European data protection standards and of the 'adequacy' issue. It considered a number of proposals to update and strengthen Israeli data protection law. Some were accepted, others rejected, based on majority and minority views.

One Schoffman proposal was to introduce a European-style definition of personal data. The proposed definition is, to all intents and purposes, the same as that found in the European Data Protection Directive. The adoption of this definition would clarify and simplify the scope of the PPA and would help to overcome the PPA's somewhat confusing relationship between sensitive and non-sensitive data. It would also bring about greater harmony with European standards.

The Schoffman Committee also proposed to bring non-computerised collections within the scope of the PPA's database provisions, bringing about equivalence with European data protection law - which does cover structured collections of non-computerised information.

The Schoffman Committee also recommended relaxing registration for 'ordinary' information-holders and concentrating on those holding specific categories of information which, in European data protection terms, would be classed as 'sensitive' – eg medical data, criminal records or information about a person's political or religious beliefs. The new registration system would also apply to databases held by list brokers.

Other recommendations adopted by the Schoffman Committee include adding the PPA to a list of statutes under which individuals can join in a class-action lawsuit –although some such claims are already actionable under current consumer protection laws. This extension would be particularly useful in cases where, for example, a data security breach has affected a large number

of people, but none of them seriously enough to warrant individual legal action. The Committee also recommended bringing in a breach-notification system, modelled on California's Security Breach Information Act 2003. ILITA would the recipient body for breach notifications, and could carry out enforcement or remedial action based on the intelligence it receives.

Schoffman suggests dealing with the issue of ILITA's independence by giving it the standing to join data protection litigation independently of the Attorney General, whilst remaining part of the Ministry of Justice

It is worth noting that the Schoffman Committee's recommendations were not intended to bring about a replication of European, or any other, data protection law. Even if all the Committee's recommendations were enacted, there would still be variation in approach between European Directive-style law and Israeli privacy law. There would still be no set of data protection principles, although, arguably, their requirements are implicit in other elements of the PPA. There would still be no 'conditions for legitimising' the processing of personal data. It is worth noting that ILITA is currently working on a wider reform of Israel's law, and on the development of a set of data protection principles.

6. What has happened since Schoffman?

Once the Schoffman Committee reported in 2007, there were a number of options for taking its recommendations forward. One option was to draft a comprehensive new bill that would, in effect, introduce a new data protection law, separate from the 'classical' privacy protection provisions of Chapter 1 of the PPA. However, the decision was taken to implement the Schoffman recommendations in a number of steps.

At the time of writing (autumn 2009), a draft 'enforcement bill' is about to be published. This is intended to upgrade ILITA's enforcement powers. Its main thrust is defining numerous new administrative sanctions and fines, which will be imposed by ILITA directly. It defines new criminal offences, and sets out special criminal inquiry powers such as accessing premises and carrying out searches. Such powers exist in today's PPA (see section 10, ann. 31A), but they will be greatly developed and expanded. In addition ILITA is initiating a data protection self-audit system as an alternative to registration. Interestingly, large database owners will also be required to produce a diagrammatic representation of their information systems, this will serve as a compliance tool for the organisation and as a regulatory one for ILITA. This approach perhaps reflects the complexity of modern information systems and the difficulty of producing a verbal description of them for registration or other compliance purposes. ILITA is following established principles of good regulation in seeking to reduce the regulatory burden, by bringing in wide exemptions for 'low-risk' organisations with a small workforce and turnover.

In terms of the other Schoffman recommendations, the Ministry of Justice and ILITA must decide whether the best course of action would be to amend the existing 'databases' chapter of the PPA or, given the radical and wide-reaching nature of some of the recommendations, to start again with a whole new data protection law. At the time of writing, the options are still being considered.

7. The Israeli supervisory authorities: Registrar of Databases and ILITA

When the PPA was enacted in 1981, it provided for the appointment of a registrar of databases. The first registrar was appointed in September of that year. The law clearly envisaged a database as being a rare and unusual thing, whose existence had to be declared to the authorities. Indeed, in 1981 the existence of a computerised database would have been fairly uncommon in Israel, as elsewhere. As was the case with various pre-Directive manifestations of European data protection law, the purpose of the registration system was a) to allow the registrar to scrutinise the data processing carried out on the database and to order any necessary remedial action and b) to further public transparency by allowing individuals to inspect the register.

It is clear that in its formative period, the office of Database Registrar was primarily concerned with the registration task itself, rather than with wider privacy issues. That said, the PPA did require the Registrar to submit a Protection of Privacy report to the Knesset, which could touch on broader issues than database registration. Indeed, the registrar of databases did expand its activity to cover awareness-raising and to establish a database supervisory team. Despite the increased activity, it is fair to say that the Registrar kept a fairly low profile, wasn't particularly active, and was mainly concerned with the bureaucratic exercise of keeping a national register of databases. Although maintaining the register will have done something to raise basic awareness, the process probably had a negligible effect on compliance by organisations, or on the protection of individuals' personal information.

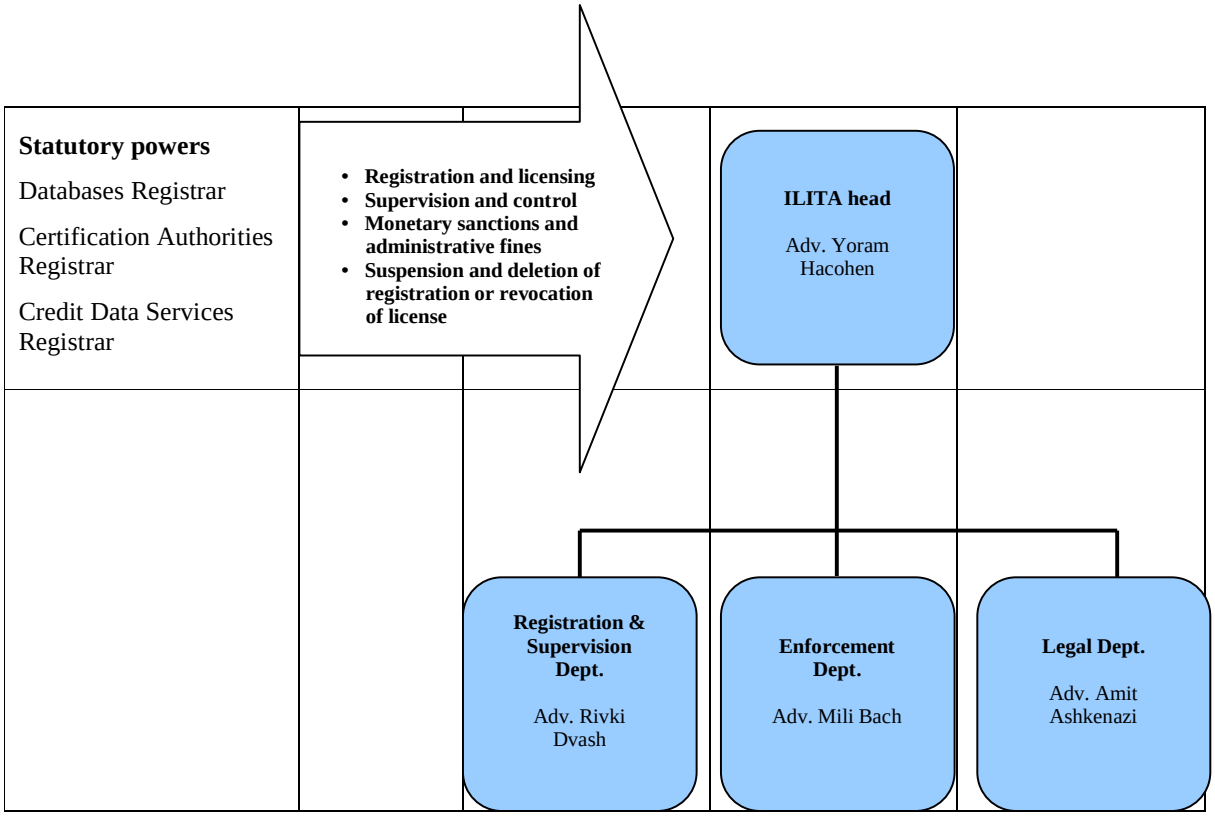
The next major development in the history of the Israeli supervisory authority was the establishment of the Israeli Law Information and Technology Authority (ILITA) in 2006. This authority is an organisational merger of three statutory law and technology regulators set up under the PPA, the Electronic Signature Act 2001 and the Credit Reporting Act 2002. Therefore ILITA carries out the Database Registrar's functions.

ILITA sits within the Israeli Ministry of Justice, with a leader who serves as both the Registrar of Databases and as ILITA's head. The creation of ILITA opened the way for a much more active supervisory authority, carrying out a more varied mix of regulatory activities, involving enforcement, complaints handling and a supervisory role, as well as maintaining a registration system. The Israeli supervisory authority is taking a path which parallels that taken by many other authorities. It is moving away from a rather technical and bureaucratic approach, focussed on registration, and is taking up a much more relevant role, dealing with practical issues in the mainstream of Israel's information society.

ILITA recruits its staff using the same channels as the mainstream Ministry of Justice. Its non-registration functions are funded by the Ministry of Justice, and its Head was appointed by a committee headed by the Director General of the Ministry of Justice. ILITA is dependent on the

Ministry of Justice for much logistical support, not least for the provision of its premises and equipment. This relationship makes logistical sense, in terms of keeping down the overheads that would otherwise be disproportionately high for an office of ILITA's size. However, ILITA's situation is not that dissimilar to some other supervisory authorities, in Europe and elsewhere, who have varying degrees of closeness to, and dependence upon, a governmental sponsoring body. Despite the logistical dependence on the Ministry of Justice, neither the Minister of Justice or the Ministry's Director General can, or are authorised to, interfere in professional decisions of the Database Registrar. This is an example of the Ministry of Justice 'hosting' an independent body. It has similar relations with bodies such as the Department of Land Registration, the Companies Registrar or the Official Receiver. In their regulatory roles, these units are not subject to the authority of the Minister of Justice or the Ministry's Director General. So, for example, the Minister of Justice or the Ministry's Director General cannot interfere in a decision to register a parcel of land, to delete a company from the Companies Registry, or to participate in a bankruptcy proceeding. The same sort of independence is afforded to the Database Registrar.

There is no doubt that ILITA is developing into an increasingly distinct, independent body within the Ministry of Justice. There is also no doubt that the law requires ILITA to regulate public sector databases, including ones controlled by government departments such as the Ministry of Justice. It is implicit in ILITA's statutory duties that it must be able to take action against government departments, and it is explicit that the PPA applies to the State.



ILITA: basic organisational structure

8. Recent ILITA activity: selected highlights

The final section of this guide to data protection in Israel is intended to give readers an overview of some of ILITA's current activities, in order to provide an understanding of how data protection law in Israel works in practice and of regulator's approach.

ILITA's inspection unit: The inspection unit was set up in 2000, but in recent times has become a lot more focused and active. Like most data protection authorities, ILITA's resources are modest in relation to the demands placed on it and the functions it is expected to perform. ILITA has therefore embarked on a similar journey to other data protection authorities, in terms of targeting its activities at areas of greatest risk. This can involve taking up sensitive issues with powerful adversaries in contentious circumstances. This has particularly been the case when regulating state institutions, where questions of data retention, excessive collection, unfair use of information or inadequate rules for disclosure to third parties have arisen. ILITA has not been afraid, either, to challenge the data handling practices of some of its largest financial institutions, for example over the disclosure of information about credit card transactions and the public availability of a register of people who have 'bounced' cheques.

Companies register: During 2008, ILITA worked with the Companies Authority in the Ministry of Justice to examine arrangements for distributing data from the Register of Companies. This came about as the result of various problems that came to light, particularly concerning the distribution of data through concessionaires. It led to the development of a supervisory framework for the legitimate distribution of data from the register. This resulted in the drafting of a law memorandum which proposes a data distribution licensing system that will enable a proper balance to be struck between privacy and the availability of information. This was put out to public consultation and the resulting memorandum is due to be presented to the Knesset this year.

Defence Ministry: In 2007 the registration of the database in the Defence Ministry's Rehabilitation Department was suspended. This was because of a failure to comply with information security requirements when outsourcing information. A follow-up meeting was held between representatives of the Defence Ministry and the Databases Registrar - this involved the Ministry providing additional information about its privacy protection procedures. The investigation showed that there were still defects in the Ministry's privacy protection procedures when outsourcing. The Databases Registrar instructed the Ministry to correct these defects and will check that this has been done.

Hospital security breach: Following a journalistic report about a security failure on an Israeli hospital's website, an inspection was carried out to determine the nature of the failure and to examine the conduct of the hospital and the company operating its website. The inspection showed that an information security failure had allowed unauthorised persons to view information about patients' appointments. The defect was corrected immediately by the company operating the site, but an examination revealed other defects in the hospital's information security policy. As a result of the Registrar's intervention, the hospital prepared an action plan for dealing with the defects, including carrying out a comprehensive risk survey. This action plan is due to be implemented by the hospital in the course of 2009, and the registrar will check that the hospital is implementing the action plan and has corrected its security problems.

Disclosure of credit card information: A complaint was received about a credit card company disclosing excessive information to a third party. The complaint concerned a claim filed by a third party against the complainant and the credit card company in respect of a particular transaction carried out by the complainant. The company attached printouts detailing the complainant's transactions over several months to its statement of defence. Each of the printouts showed the complainant's account number, a list of the transactions, payments for other transactions, details of the credit limit and other data. It was shown that the credit card company had disclosed excessive and unnecessary information, because only information about one transaction with one business was relevant to the proceedings. The disclosure therefore constituted an infringement of privacy under section 2 of the PPA. The company was requested to inform the registrar of the steps it would take in order to ensure that there would be no recurrence.

9. The adequacy of Israeli data protection law

The European Data Protection Directive places restrictions on the transfer of personal data outside the European Economic Area (EEA). However, personal data can be transferred to a country outside the EEA provided the European Commission has decided that the law of the country in question provides an adequate level of protection for personal data. Following a detailed assessment of Israel's data protection law, at its December 2009 meeting, the Article 29 Working Party (which consists of European data protection authorities) deemed Israel's law to be 'adequate'. This means that a data controller within the EEA can now transfer personal data to Israel without breaching the Directive's restriction on the transfer of personal data to third countries.

10. Conclusion

There are undoubtedly differences between Israeli data protection law and that found in Europe and elsewhere. However, there is no doubt that Israel has a fully functioning data protection system, operating against the backdrop of a democracy with an independent judiciary. This has been recognised in the European Commission's recent decision to deem Israel's data protection law to be 'adequate'. In ILITA, Israel has an active and committed regulatory authority that analyses its society's privacy risks intelligently, deals with the public's complaints diligently and sympathetically and is not afraid to take on powerful adversaries when it needs to do so.

Levels of data protection awareness in Israel are probably low relative to countries in Europe. However, ILITA is working hard to raise awareness, by taking the right cases, publicising the positive outcomes of their work and developing a regulatory mix of positive engagement with the willing and firm action against the deliberately non-compliant. It is clear that ILITA sees data protection in Israel as becoming a more important part of country's culture, as its information society develops and expands. It is also clear that ILITA is very keen to learn from the experiences of other data protection authorities. It is an exceptionally open-minded and receptive organisation.

Respect for personal privacy is a well established part of Israel's culture. Its roots go back to the founding of the state. Israel has a population that is certainly not afraid to take action when it feels its privacy rights are being infringed. There is certainly no prospect of ILITA's workload diminishing in the immediate future.

I Bourne – Head of Data Protection Projects, Information Commissioner's Office, UK
January 2010