

September 2014

IP RIGHTS IN DATA HANDBOOK

Protecting and exploiting IP in data, big data and databases internationally





EDITORS



John Wilks, Editor
Partner
T +44 (0)20 7796 6288
M +44 (0)7796 15 8896
john.wilks@dlapiper.co.uk



Alec Christie, Co-Editor
Partner
T +61 2 9286 8237
alec.christie@dlapiper.com



Christopher Götz, Co-Editor
Senior Associate
T +49 221 277 277 392
christopher.goetz@dlapiper.com

INTRODUCTION

In the era of Big Data, no ambitious business can afford to live without a strategy for the acquisition, protection and exploitation of the data upon which it depends. The laws enabling data to be protected and exploited are becoming ever more important to businesses, no matter the sector in which they operate. Yet, not surprisingly, laws relating to IP protection of data and databases vary significantly among jurisdictions. This naturally poses a challenge to any business looking to protect and exploit data on a cross-border basis.

This guide was devised to provide an overview of the IP and related rights affecting data and databases. This, our second edition of the IP Rights in Data Handbook, now covers 20 jurisdictions and includes for each country top tips from local professionals on how best to exploit Big Data.

How this Handbook Works

This Handbook provides a high-level summary, with links to relevant sources, of the different types of protection available for data and databases in 20 key global jurisdictions. For each jurisdiction, we consider three categories of database which may benefit from protection: original databases; databases in which investment has been made; and confidential databases.

As database law is only partly harmonised in the EU, we offer, in addition to a section on the EU, separate sections on eight representative EU jurisdictions (Austria, Belgium, France, Germany, Italy, The Netherlands, Romania, Spain and the UK). To assist you in navigating our European content and avoiding repetition, there are cross-references between the [EU section](#) and the national sections.

Data privacy law is not the focus of this guide. However, we understand that there is an overlap in that data privacy laws do limit both database owners' ability to exploit data and database users' ability to use it. We have therefore very briefly summed up the scope of the data privacy/data protection regime in each country. More detailed information on data privacy/data protection regimes in 72 jurisdictions can be found in our separate [Data Protection Laws of the World Handbook](#).

The DLA Piper Rights in Data Team

The global DLA Piper Rights in Data Team is made up of professionals experienced in dealing with the business IP issues that arise in connection with data and databases. We pool and share our extensive knowledge of many types of operators (both public and private) across many sectors and jurisdictions. We have market-leading experience in such related areas as IT, media, sport, confidentiality, competition law and data privacy/data protection. As we are based in offices across the globe, we are able to work efficiently and effectively on cross-border projects and litigation involving data supply and use. A few snapshots of our experience from around the world are on page 4; details of our extensive experience, both at the global and local levels, are available on request.

CONTENTS AND AT-A-GLANCE SUMMARY

Section A: Global Overviews

Overview Topic	Page No.
Snapshots of our experience.....	05
Summary of key issues for database owners.....	06
Top tips for database owners.....	07
Top tips for those who exploit big data	09

Section B: Summaries by Jurisdiction

Jurisdiction	Page No.	Are original databases protected?	Is investment in databases enough to secure protection?	Does a claim for misusing confidential information exist?	Is personal data subject to protection?	Key DLA Piper Contacts
Australia	10	✓	x	✓	✓	Alec Christie Caroline Atkins
Austria	15	✓	✓	✓	✓	Sabine Fehringer
Belgium	18	✓	✓	✓	✓	Patrick Van Eecke Alexis Fierens
Brazil	22	✓	x	✓	✓	Antonio Murta Marcelo Goyanes
China	25	✓	x	✓	✓	Richard Wageman
EU	29	✓	✓	✓	✓	See EU law section
France	34	✓	✓	x	✓	Jeanne Dautier Stephane Lemarchand
Germany	36	✓	✓	✓	✓	Jan Pohle Christopher Goetz
Hong Kong	40	✓	x	✓	✓	Scott Thiel Edward Chatterton
India	45	✓	✓	x	✓	Sajai Singh Probir Roy Chowdhury Soumya Patnaik

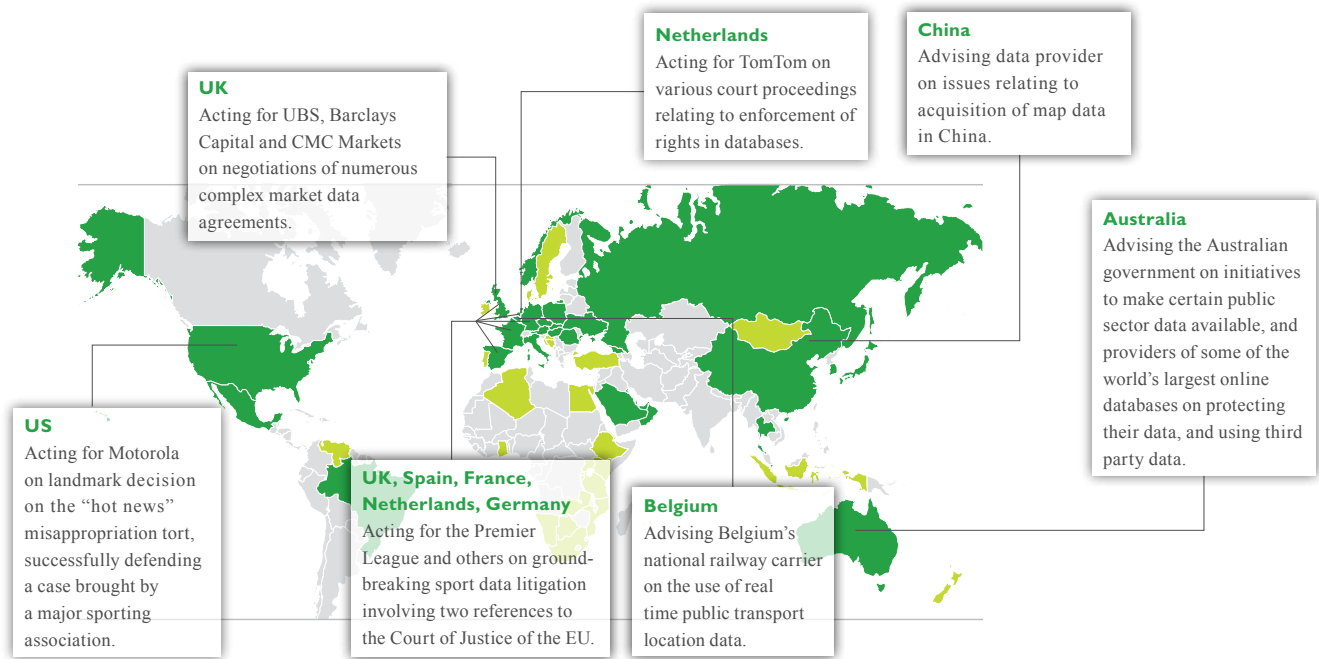
Jurisdiction	Page No.	Are original databases protected?	Is investment in databases enough to secure protection?	Does a claim for misusing confidential information exist?	Is personal data subject to protection?	Key DLA Piper Contacts
Italy	49	✓	✓	x	✓	Roberto Valenti Stefania Baldazzi
Japan	52	✓	x	x	✓	Henry Koda
The Netherlands	56	✓	✓	✓	✓	Alexander Tsoutsanis Robin de Wit
Romania	60	✓	✓	x	✓	Cosmina Simion Laura Leanca
Singapore	63	✓	x	✓	✓	John Goulios Yvonne Lee
South Africa	67	✓	✓	✓	✓	Preetta Bhagattjee Simone Gill
South Korea	73	✓	✓	✓	✓	Kwang Bae Park Hwan Kyoung Ko
Spain	77	✓	✓	x	✓	Diego Ramos
Turkey	79	✓	✓	✓	✓	Gökhan Gökçe Burak Ozdagistanli
UK	82	✓	✓	✓	✓	John Wilks Jim McDonnell
USA	85	✓	x	✓	✓	Andrew Deutsch James Halpert

This handbook is provided to you as a courtesy, and it does not establish a client relationship between **DLA Piper** and you, or any other person or entity that receives it. It provides a general overview of the law governing rights in data/databases currently in force in 20 jurisdictions. It is a general reference document and should not be relied upon as legal advice. The application and effect of any law or regulation upon a particular situation can vary depending upon the specific facts and circumstances, and so you should consult with a lawyer regarding the impact of any of these regimes in any particular instance. **DLA Piper** accepts no liability for errors or omissions appearing in the handbook. Please note that IP law is dynamic, and the legal regime in the countries surveyed could change. No part of this publication may be reproduced or transmitted in any form without the prior consent of the **DLA Piper**.

© 2014 **DLA Piper UK LLP**



SNAPSHOTS OF OUR EXPERIENCE AROUND THE GLOBE...



DLA PIPER

ALGERIA Algiers	AUSTRALIA Brisbane Canberra Melbourne Perth Sydney	BRAZIL São Paulo	CHINA Beijing Hong Kong Shanghai	CZECH REPUBLIC Prague	FRANCE Paris	GERMANY Berlin Cologne Frankfurt Hamburg Munich	HUNGARY Budapest	INDONESIA Jakarta	IRELAND Dublin	ISRAEL Tel Aviv	ITALY Milan Rome	JAPAN Tokyo	KUWAIT Kuwait City	LUXEMBOURG Luxembourg	MEXICO Mexico City	NETHERLANDS Amsterdam	NORWAY Oslo	OMAN Muscat	POLAND Warsaw	QATAR Doha	ROMANIA Bucharest	RUSSIA Moscow St. Petersburg	SAUDI ARABIA Riyadh	SINGAPORE Singapore	SLOVAK REPUBLIC Bratislava	SOUTH KOREA Seoul	SPAIN Madrid	THAILAND Bangkok	TURKEY Istanbul	UKRAINE Kyiv	UNITED ARAB EMIRATES Abu Dhabi Dubai	UNITED KINGDOM Birmingham Edinburgh Leeds Liverpool London Manchester Sheffield	UNITED STATES Albany Atlanta Atlantic City Austin Baltimore Boston Chicago Dallas Houston Los Angeles La Jolla Miami Minneapolis	New York Northern Virginia Philadelphia Phoenix Raleigh Sacramento San Diego San Francisco Seattle Silicon Valley Tampa Washington, DC Wilmington
--------------------	---	---------------------	---	--------------------------	-----------------	--	---------------------	----------------------	-------------------	--------------------	------------------------	----------------	-----------------------	--------------------------	-----------------------	--------------------------	----------------	----------------	------------------	---------------	----------------------	------------------------------------	------------------------	------------------------	-------------------------------	----------------------	-----------------	---------------------	--------------------	-----------------	--	--	---	---

RELATIONSHIP FIRMS

ALGERIA Algiers	ETHIOPIA Addis Ababa	GHANA Accra	INDONESIA Jakarta	IRELAND Dublin	ISRAEL Tel Aviv	ITALY Milan Rome	JAPAN Tokyo	KUWAIT Kuwait City	LUXEMBOURG Luxembourg	MEXICO Mexico City	NETHERLANDS Amsterdam	NORWAY Oslo	OMAN Muscat	POLAND Warsaw	QATAR Doha	ROMANIA Bucharest	RUSSIA Moscow St. Petersburg	SAUDI ARABIA Riyadh	SINGAPORE Singapore	SLOVAK REPUBLIC Bratislava	SOUTH KOREA Seoul	SPAIN Madrid	THAILAND Bangkok	TURKEY Istanbul	UKRAINE Kyiv	UNITED ARAB EMIRATES Abu Dhabi Dubai	UNITED KINGDOM Birmingham Edinburgh Leeds Liverpool London Manchester Sheffield	UNITED STATES Albany Atlanta Atlantic City Austin Baltimore Boston Chicago Dallas Houston Los Angeles La Jolla Miami Minneapolis	New York Northern Virginia Philadelphia Phoenix Raleigh Sacramento San Diego San Francisco Seattle Silicon Valley Tampa Washington, DC Wilmington
--------------------	-------------------------	----------------	----------------------	-------------------	--------------------	------------------------	----------------	-----------------------	--------------------------	-----------------------	--------------------------	----------------	----------------	------------------	---------------	----------------------	------------------------------------	------------------------	------------------------	-------------------------------	----------------------	-----------------	---------------------	--------------------	-----------------	--	--	---	---



RIGHTS IN DATA HANDBOOK SUMMARY OF KEY ISSUES FOR DATABASE OWNERS

RIGHTS IN DATA	PROTECT	Are there applicable IP rights?	Database right (in EU): if sufficient investment in obtaining etc
			Copyright: if sufficient originality
			Importance of clear chain of ownership
		Is the database confidential?	Can be key for non public information
			Importance of contractual confidentiality provisions
		Has an audit of data been conducted?	Work out what data is held
		Establish what rights protect it and what rights have been licensed	
		Establish who owns those rights	
	EXPLOIT	What is scope of licence?	Purposes for which use permitted
			Where and when use is permitted
			Extent to which sub-licensing allowed
		What are the key commercial terms?	Financials
			Definition of supplied data
			Exclusivity
	What practical issues arise around data provision and use?	Data security/confidentiality issues	
Technical specifications of data format etc			
Potential competition/antitrust issues			
ENFORCE	Is data use/infringement monitored?	Audit rights and practical controls on licensees	
		Targeted seeding to catch infringers	
		Use of specialist monitoring/investigative services	
	What potential claims are there?	IP-copyright, database right, trade marks	
		Breach of confidence	
		Breach of contract	
What is your litigation strategy?	Aim may be to set an example or just stop this infringer		
	Choosing targets and forum carefully		
	Need to keep costs proportionate		



TOP TIPS FOR DATABASE OWNERS

IP PROTECTION

- Identification of the author is very important for copyright protection of databases. Therefore records identifying the author and history of the creation of the database must be kept.
- Ensure that contracts with third parties who undertake tasks in relation to a database on your behalf (e.g. collating, gathering, organising information/data) are clear on the ownership of IP and confidential information in the database.
- Audit the data you own: consider the range of potential rights available to protect the data, and take steps to ensure you benefit from such protection, including obtaining IP assignments from all those who could potentially own the rights in the database.
- Audit the data you consume:
 - Are appropriate licence terms in place?
 - Do those using the data know what those licence terms are?
 - Does the licensor own all the relevant rights?
- Include “seeds” (deliberately inserted fake information) in your database, so that you can trace and prove infringement.
- Trade marks may also be an appropriate further protection for certain types of data (such as financial indices).

CONTRACTUAL

- Get expert advice early on: regardless of whether you have an existing database or plan to create a new one choosing the right business model is critical, not only for maximizing revenue, but also for maximizing legal protection.
- Where possible, establish strong protection rights through individually negotiated contracts.
- Ensure that adequate contractual protections are in place/accepted prior to or at the time of third parties accessing your database, including:
 - licensing provisions;
 - contractual restraints on use; and
 - contractual requirements to return physical property on which the database resides on termination.
- Publicly available databases should have appropriate terms of use to ensure users have appropriate contractual obligations in relation to the information they access/use. In particular, contractual provisions against disclosure/dissemination should be visible to the user and you should ensure the user’s assent to those conditions can be clearly evidenced.
- Consider (particularly in the case of sophisticated corporate users) whether to make contractual rights in the database subject to the laws of a country with stronger database protection (such as EU countries), if either the provider or user has some connection to that country.



CONFIDENTIALITY

- Obtain local advice on how best to protect your confidential information (law on this varies considerably from jurisdiction to jurisdiction).
- Confidential databases should only be communicated/ disclosed with a clear message regarding the confidential nature of the database, and that disclosure is subject to the obligation to keep the database confidential.
- Specify confidentiality restrictions in agreements which those who wish to access must accept; consider providing specific penalties in case of breach of these restrictions.
- Also enter into specific non-disclosure agreements with employees, partners, consultants and anyone else who may have access to your databases.
- Establish strong technological protection (eg passwords) against unauthorized access or copying. Frequently update databases, where possible, so that if a user violates the terms of an agreement, its access can be terminated, and the value of any data it still possesses will diminish over time (ie as it becomes out of date).

DATA PRIVACY

- Always consider personal data protection/privacy laws applicable in the relevant jurisdictions, such as consent, permissible use, transferability, storage rights, etc when acquiring a database.



TOP TIPS FOR THOSE WHO EXPLOIT BIG DATA

IP PROTECTION

- Do not underestimate the extent to which privacy laws differ between different territories. Consider which laws will apply early on to ensure you can develop a compliant strategy for exploiting Big Data.
- Fully assess the impact of data protection laws at all stages, from collection through internal processing to exploitation; and take necessary steps to ensure compliance.
- Ensure transparency from the time of collection (i.e. notify individuals of likely uses of their information for Big Data analytics in the privacy statement/privacy policy at the time of collection and consider re-notification/re-consent at appropriate times). Remember, privacy notification/consent obligations on you may arise on re-identification (or the possibility of re-identification) of third parties who originally provided “anonymous” data.
- Where data is collected from a third party data provider, businesses should contractually require that third party data provider to be responsible for ensuring that the data is acquired and provided legally. Where data is collected by the business itself, the business should be aware of the types of data being collected, since some of the data may, in some jurisdictions, require additional compliance measures. For example:
 - additional obligations apply to collection and use of “sensitive personal data” (such as medical data) in the EU; and
 - if the data collected is (or is likely to be regarded as) a state secret, any access, use or transfer of such data should be restricted and monitored as required by local law.
- In addition to privacy, do not forget that third parties may potentially have IP rights over elements of the data you have gathered (in particular it may be subject to database right): evaluate whether they do, and if so what rights exist and who owns them.



- Australia
- Austria
- Belgium
- Brazil
- China
- EU
- France
- Germany
- Hong Kong
- India
- Italy
- Japan
- The Netherlands
- Romania
- Singapore
- South Africa
- South Korea
- Spain
- Turkey
- UK
- USA

I. AUSTRALIA

KEY CONTACTS



Alec Christie
 Partner
 T +61 2 9286 8237
 alec.christie@dlapiper.com



Caroline Atkins
 Partner
 T +61 2 6201 8789
 caroline.atkins@dlapiper.com

ORIGINAL DATABASES

Protected? Original databases may be protected in Australia by copyright as a ‘literary work’ (defined to include ‘a table, or compilation, expressed in words, figures or symbols’; databases may be protected as electronic ‘compilations’) under the Australian *Copyright Act 1968 (Cth) (Copyright Act)*.

Ownership The database author(s) are the first owner(s) of the copyright, unless made by an employee or employees within the scope of the author’s employment (in which case the employer is the first owner).

Pre conditions The database must be ‘original’ in the sense that its creation must involve ‘independent intellectual effort’ and/or the exercise of ‘sufficient effort of a literary nature’. Also, the database must have been reduced to material form (e.g. written down or stored on a disk). However, copyright does not protect the underlying data (i.e. facts or base information). If copyright arises, in the case of a database, it is the (non-trivial/non-obvious) form of the ‘compilation’ that is protected not the underlying data itself. A copyright notice is not required nor is there any requirement to register the copyright as Australia does not have a copyright register.

May cover Marketing databases with a complex structure (i.e. non-obvious format/choice of data types) based on an assessment of customer/business needs.

Unlikely to cover Telephone directories, databases structured on an obvious (e.g. alphabetical) basis, databases which are produced by an automated computer process.

Duration Copyright protection, if it arises, will apply automatically once an original database exists and is reduced to a material form. Protection lasts for 70 years after the end of the calendar year in which the author (or the last author, if the database is a work of joint authorship) dies.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Scope of Protection Copyright is infringed by (without authorisation of the copyright owner) doing acts comprised in the copyright (e.g. reproducing the database, publishing the database, communicating the database to the public), authorising others to do the acts comprised in the copyright or by the sale or importation of unauthorised copies in Australia. Acts done in relation to a substantial part of the copyrighted work are deemed to be done in relation to the whole (e.g. infringement occurs if a substantial part of the database is reproduced without authorisation). There are a number of fair dealing exceptions, including use for research, study, criticism or review, reporting news and parody or satire. The Australian Law Reform Commission has recently completed an inquiry into Copyright and the Digital Economy and has recommended that the fair dealing exceptions be replaced by a more flexible fair use regime.

Remedies include. Injunctions (interim and final), account of profits, damages, additional damages (e.g. due to flagrancy of infringement) and/or delivery up for destruction.

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Databases in which investments have been made do not receive protection beyond the protections described above and below or those under applicable contractual obligations (if any). The High Court of Australia has indicated that the commercial value of (or investment made in creating) a database is not relevant to subsistence of copyright. Additional contractual terms on access, use etc are the most effective way to protect databases which do not qualify for copyright protection.

CONFIDENTIAL DATABASES

Protected? The obligation to maintain confidence in a database can be enforced in the areas of contract and equity. A contractual obligation to maintain confidence may arise as an express or implied term within a contract and may be enforced for an actual or threatened breach of that obligation. The equitable obligation of confidence arises where no contract is present but rather where confidential information is imparted in circumstances giving rise to an obligation of confidentiality.

Ownership The right to protection belongs to the confider of the database, but only in circumstances where the recipient of the information contained in the database owes the confider an obligation to keep the information confidential (i.e. only if a reasonable person in the position of the recipient would understand that the information was given in confidence). It is therefore recommended that any such obligation of confidence be clearly specified in relevant documentation in the contract and T&Cs.

Pre conditions The information contained in the database will not be protected under the law of confidential information unless: (i) the information has the necessary quality of confidence; (ii) the owner has taken sufficient steps to preserve the confidentiality of its information; and (iii) a reasonable person in the position of the recipient would understand that the information was given in confidence.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

May cover Databases containing information which is largely unknown outside the confider's business.

May not cover Databases which consist of readily available information/are not difficult for others to duplicate or which are licensed on terms which do not impose obligations of confidentiality.

Duration The protection arises from the time the obligation of confidence arises (i.e. on providing the confidential database) and lasts until the obligation ceases (e.g. usually until the information passes into the public domain).

Scope of protection The usual elements to establish breach of confidence are (in addition to those mentioned under "Pre-Conditions" above): (i) the information must have been imparted in circumstances importing an obligation of confidence; and (ii) there must be an unauthorised use (or threatened unauthorised use) of that information to the detriment of the party which communicated it.

Remedies Remedies for breach of the equitable obligation of confidence include compensation, injunctions and declarations. Where the obligation arises in contract, a party may seek damages for breach of contract and, in some cases, injunctions to stop offending behaviour.

PERSONAL DATA

Is personal data given particular protection? The collection, use and disclosure of 'personal information' is protected under the *Privacy Act 1988 (Cth) (Privacy Act)*, which establishes and regulates a national scheme for the collection, use and disclosure of personal data by private and Federal public entities. From 12 March 2014 these entities need to comply with the Australian Privacy Principles (APPs). Corporations can face civil penalties of up to \$AUD 1.7 million for serious or repeated breaches of the APPs.

Who can rely on it? The individual who is the subject of the personal information.

What data? Personally identifiable information or "personal information" under the Privacy Act, is defined as information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent or can reasonably be ascertained.

Scope of protection The Privacy Act regulates the collection, storage, access, use and disclosure (including transfer) of personal information. Generally, personal information can only be used for the notified purpose for which it was collected (the 'original purpose').

A key point to note is that the Privacy Act requires individuals to be provided with notice regarding prescribed matters such as who is collecting their information, how their information will be used and to whom it will be disclosed. Notice must be provided at or before the time of collection. Where sensitive information (such as health records, race or sexual preference etc.) is collected or where personal information is used for a purpose different to the original purpose for which it was collected, individuals must give consent to this collection or use.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Data can also be collected in a de-identified form, meaning that the information does not identify individuals. Currently, the use of de-identified information in Australia is unregulated. However, as soon as such information is applied in such a way that it is re-identified (or becomes re-identifiable), its use is subject to the obligations imposed by the *Privacy Act*.

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

There are no other forms of general protection. However, there are some sector specific laws which regulate the handling of certain types of data. For example, the *Privacy Act* also contains provisions that regulate consumer credit reporting and the *Telecommunications Act 1997* (Cth) contains provisions that regulate the handling of telecommunications information held by telecommunications carriers and others (e.g. emergency call persons).

SIGNIFICANT RECENT CASES

IceTV Pty Limited v Nine Network Australia Pty Limited¹ This case concerned weekly TV schedules and originality of TV program guides produced from Channel Nine’s database. IceTV used portions of Nine’s television program guide in compiling its own electronic guide. The High Court held that IceTV did not infringe copyright. In order to be protected as a ‘compilation’ (i.e. a literary work) the work must be ‘original’ in the sense that its creation must involve ‘independent intellectual effort’ and/or the exercise of ‘sufficient effort of a literary nature’ by humans².

Telstra Corporation Limited v Phone Directories Company Pty Ltd³ The Full Federal Court held that copyright did not subsist in the White Pages or Yellow Pages directories. This case highlights the difficulty of a claim to copyright in a literary work which is compiled by an automated process. Keane CJ stated: “The dicta in *IceTV* shifted the focus of inquiry away from a concern with the protection of the interests of a party who has contributed labour and expense to the production of a work, to the “particular form of expression” (i.e. ‘creative spark’) which is said to constitute an original literary work and to the requirement of the [Copyright] Act that the work originates with an author or joint authors from some independent intellectual effort”. Labour (often referred to as ‘industrious collection’ or ‘sweat of the brow’) is relevant only to show that the compilation originated from the author (rather than being copied) not to show sufficient independent intellectual or literary effort.

UPCOMING LEGISLATIVE CHANGES

In relation to databases, some commentators have suggested that the recent decision would lead to calls for introduction of sui generis rights for databases in Australia. Further, in *Telstra Corporation Limited v Phone Directories Company Pty Ltd* (which followed *IceTV*), Justice Gordon suggested that legal protections for databases (such as those set out in the EU Database Directive 96/9) should be addressed by the Australian Parliament ‘without delay’. However, we are unaware of any significant public advocacy for the introduction of such rights.

¹ (2009) 239 CLR 458.

² See *IceTV* at [33], [99], and [187] [188]

³ (2010) 194 FCR 142.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Amendment Act)* strengthened existing protections for personal information in Australia. The Amendment Act has made various changes to the Privacy Act, including the restriction of the use of personal information for direct marketing purposes and restrictions on cross-border disclosure of personal information. The changes commenced on 12 March 2014.

TOP TIP FOR DATABASE OWNERS

Protection of databases in Australia is assisted by ensuring that adequate contractual protections are in place/accepted prior to or at the time of accessing the database, including:

- licensing provisions
- contractual restraints on use
- contractual requirements to return physical property on which the database resides

TOP TIP FOR THOSE WHO EXPLOIT BIG DATA

- Ensure transparency from the time of collection (i.e. notify individuals of likely uses of their information for Big Data analytics in the privacy statement/privacy policy at the time of collection and consider re-notification/consent at appropriate times) and remember your privacy re-notification obligations on re-identification of third party provided “anonymous” data.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

2. AUSTRIA

KEY CONTACTS



Sabine Fehringer
Partner
T +3 | 513 78 1453
sabine.fehringer@dlapiper.com

The law is part-harmonised with general EU law (see [EU section](#)); in this section we therefore only highlight areas which differ from the EU-wide position.

ORIGINAL DATABASES

Protected? Databases are subject to copyright protection as a “database”. Subject to the [EU-wide EU-Database Directive 96/9](#) (see [EU section](#)), implemented by the *Urheberrechtsgesetz* (Austrian Copyright Act) – “**UrhG**”, section 40 f, para. 1 of which defines “database” as “collection of works, data or other independent elements which are systematically or methodically arranged”.

Pre-conditions The database must be the “*author’s own intellectual creation*” (“*eigentümliche geistige Schöpfung*”) in respect to the selection or arrangement of its elements; this is implemented by Section 40 f para. 2 UrhG.

May cover Lexicon for medicine on the internet or databases with a complex structure.

Unlikely to cover Telephone directories and a collection of laws on CD-ROM.

Remedies include In instances of intentional infringement there are potential criminal sanctions, including imprisonment of up to six months or a fine (Section 91 Para 1 UrhG). If intentional infringement is on a commercial basis (“*gewerbsmäßig*”), the sanctions can be imprisonment of up to two years or a fine (Section 91 Para 2a UrhG).

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Protected? Yes, under the Database Directive which is implemented in Austria by Section 76 c *et. seq.* UrhG (see [EU section](#)).



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Remedies include: The remedies for infringement are broadly the same as for copyright, as above.

CONFIDENTIAL DATABASES

Protected? It is possible for confidential databases to be protected as business or trade secrets and confidential information, in particular Section 11 of the Austrian Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb* – “UWG”), which penalizes the disclosure of trade and business secrets by an employee, or Section 123 Austrian Criminal Code (*Strafgesetzbuch* – “StGB”), which penalizes spying on business or trade secrets for purposes of exploitation or publication. Furthermore, takeover of a competitor’s database may also constitute an unfair commercial practice under Section 1 UWG (as unfair use of a competitor’s asset).

Ownership The law in this area protects the owner of the business to which the business and trade secrets belong.

Pre-conditions Protection will arise where there are “unauthorised communications”, which includes:

1. communication of a business or trade secret (facts, circumstances and procedures, which are not obvious, and only accessible to a limited circle of persons and with regard to which the right holder has a legitimate interest not to make them public);
2. by an employee of a business, who was entrusted with or who had access to such business or trade secret during the course of the employment relationship; and
3. for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business (Sections 11, 12 UWG).

May cover Customer databases, databases of a company’s commercial or technical knowhow, databases of product ingredients.

May not cover Data which is published or licensed on terms which do not impose confidentiality obligations.

Duration The protection arises from the time the obligation of confidentiality arises, and will last until the obligation ceases (e.g. usually until the information passes into the public domain).

Scope of Protection See above under “preconditions”.

Remedies Potential remedies in this area include criminal sanctions (Section 121 et seq. StGB – either imprisonment or fines). Industrial espionage by employees or others and unauthorised exploitation of trade and industrial secrets (Section 13 UWG) can also give rise to civil law liability (claims for damages). Other relevant remedies are cease and desist orders which can be claimed pursuant to the UWG.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

PERSONAL DATA

See [EU section](#). The use of “personal data” is subject to the Austrian [Data Protection Act 2000 – “DSG 2000”](#), which implements the Data Protection Directive.

Who can rely on it? Individuals, but also legal persons, whom the data refer to (i.e. who are the “data subjects” as defined in EU law).

What Data? The definition corresponds to European law. In practice, in addition to usual examples (e.g. name, address, social security number etc.), in Austria, other information related to a person, such as opinions or judgements, are also considered personal data, i.e. the definition is interpreted broadly.

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

Generally, no. With regard to personal data collected by the state and other public bodies, there are specific provisions within the DSG 2000. Sensitive data and data relevant to criminal law are subject to stricter protection.

SIGNIFICANT RECENT CASES

Austrian Supreme Court, 12. 6. 2007, 4 Ob 11/07g – EDV Firmenbuch III – This decision is the third and latest in a row of Supreme Court decisions assessing the Austrian Companies’ Register as a *sui generis* protected database. According to the Supreme Court, since the on-going updating of the Companies’ Register is to be qualified as costs of “collection, review or presentation” of the contents of the database, the Companies’ Register is a database in which a material investment has been made and therefore subject to protection pursuant to Section 76d UrhG.

UPCOMING LEGISLATIVE CHANGES

None, other than those mentioned in the [EU section](#).

TOP TIP FOR DATABASE OWNERS

Ensure all disclosures of confidential information are subject to prior signature of an appropriate NDA. Such NDA should in particular include a contractual penalty for confidentiality breaches.

TOP TIP FOR THOSE LOOKING TO EXPLOIT BIG DATA

Consider local data protection law when devising a strategy for big data exploitation.



- Australia
- Austria
- Belgium**
- Brazil
- China
- EU
- France
- Germany
- Hong Kong
- India
- Italy
- Japan
- The Netherlands
- Romania
- Singapore
- South Africa
- South Korea
- Spain
- Turkey
- UK
- USA

3. BELGIUM

KEY CONTACTS



Patrick Van Eecke
Partner
T +32 2 500 1630
patrick.vaneecke@
dlapiper.com



Alexis Fierens
Lead Lawyer
T +32 2 500 1592
alexis.fierens@dlapiper.com

The law is part harmonised with general EU law (see [EU section](#)); in this section we therefore only highlight areas which differ from the EU-wide position.

ORIGINAL DATABASES

See [EU section](#).

Protected? The EU-wide Database Directive is implemented in Belgium by articles *20bis*, *20ter* and *20quater* of the Belgian Act of 30 June 1994 on copyright and related rights (“Copyright Act”), pursuant to which copyright protection is granted to an original database.

In respect of databases created by an employee or a public servant in the execution of his duties or following his employer’s instructions, the Belgian legislator has made use of the possibility granted under recital 29 of the Database Directive. As a result and subject to contrary contractual or statutory provisions, the employer shall exclusively be entitled to exercise all economic rights in the database so created in the non-cultural sector.

Remedies Right holders of original databases are entitled to the same remedies that are granted to any other copyright holder, warranting both (interim and final) injunctive and monetary relief, as set out under Chapter VIII of the Copyright Act. Monetary relief also entails the possibility to set the damages as a lump sum as well as the possible delivery up to the claimant of infringing goods and, in appropriate cases, of the materials and tools principally used in the creation or manufacture of these goods. In case of a bad-faith infringement, monetary relief also entails the possibility to claim payment of unfair profits made.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

See [EU section](#).

Protected? The EU-wide Database Directive is implemented in Belgium by the Act of 31 August 1998 on the legal protection of databases (“Database Act”), pursuant to which *sui generis* protection is granted to the content of certain databases.

Article 8 of the Database Act, in line with article 8.1 of the Database Directive, provides that the maker of a database which is made available to the public in whatever manner, may not prevent the lawful user of the database (or of a copy or part thereof) from extracting and/or re-utilizing insubstantial parts of its (or of that part’s) contents, evaluated qualitatively and/or quantitatively, for any purposes whatsoever. However, pursuant to articles 9 and 10 of the Database Act, such lawful user may still not perform acts which conflict with normal exploitation of the database or unreasonably prejudice the legitimate interests of the maker of the database and may not cause prejudice to the holder of a copyright or related right in respect of the works or subject matter contained in the database.

In addition, article 7 of the Database Act, which implements the options suggested in article 9 of the Database Directive, provides a limited number of legal exceptions to the exclusive database rights.

Remedies The remedies provided under articles 12^{quater} to 12^{sexies} of the Database Act are very similar to the remedies put at the disposal of the copyright holder, as described above.

CONFIDENTIAL DATABASES

As is the case in some other jurisdictions, such as in The Netherlands and France, there is no general legal right as such to prevent the misappropriation, misuse or disclosure of confidential information, other than via contractual obligations (such as non-disclosure agreements or otherwise).

However, in particular circumstances and relationships, various laws do provide for protection of confidential information, including confidential databases that contain trade or industrial secrets. These include (i) article 11 of the Act of 15 June 2006 regarding public contracts and certain contracts for works, supplies and services, (ii) article 17 (3) of the Act of 3 July 1978 on employment contracts and (iii) article 309 of the Criminal Code.

Also, more generally and dependent on the circumstances of the case, the common legal obligations to act in good faith in the context of a contractual relationship (article 1134 of the Civil Code) or, outside of such relationship, to act prudently (i.e. the principle of tort liability under article 1382 of the Belgian Civil Code or, in a commercial context, article VI.104 of



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

the new Code on Economic Law), whether or not in combination with article 39 of TRIPs, may serve as a possible legal ground for a claim in case of disclosure or misappropriation of confidential information as a result of which damages are suffered.

PERSONAL DATA

See [EU section](#). The handling of “personal data” is subject to the EU Data Protection Directive. 95/46, which has been implemented in Belgium by the Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data.

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

In general terms, there are no other types of protection for data or databases. However access to public data is governed by the Act of 7 March 2007 implementing Directive 2003/98/EC of the European Parliament and the Council regarding the re-use of public sector information.

SIGNIFICANT RECENT CASES

Select Human Resources – The court of appeal of Ghent, after a *prima facie* evaluation in the context of confiscation proceedings (*saisie-contrefaçon*), was of the opinion that an HR company’s data files such as reporting schedules and a list of vacancies, which it claimed to constitute a database, were no more than a by-product of its main activity, and that no substantial investment had been made, in qualitative or quantitative terms, in the obtaining, verification or presentation of the data contents. According to the court’s findings, investments were made in the various elements of the data contents, which enable the company to work efficiently. However, the files as such do not constitute a database within the meaning of the Database Act and the investment made did not relate to the functioning of the database itself. Thus, the court further defined the object of database protection, as laid down in article 7 of the Database Directive, and emphasized the importance of the difference between (protected) investments made in the obtaining, verification or presentation of the contents of the database on the one hand and (unprotected) investments made in the creation of the elements that constitute the contents of the database on the other hand. (Court of Appeal Ghent 14 November 2011).

Trends Top 100,000 – The court of appeal of Antwerp found that the obtaining, verifying and updating, on a yearly basis, by a financial-economic magazine, of data contained in a “top 100,000-list” of Belgian companies, takes time and money and therefore necessitates a substantial investment. Given the amount of fictitious addresses acquired across the entire database, the magazine publisher had indeed proved that at least a substantial part of the database was extracted and re-utilized. (Court of Appeal Antwerp 24 September 2007).



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Bustour – The court of appeal of Brussels considered that the mapping out of a bus route of tourist attractions does not constitute the expression of the intellectual creation of its author and is thus not a copyright protected form. Such mapped geographic route, which runs over a series of attractions and which is accompanied by an explanatory text, might constitute a collection of data, but is not accessible in a way that differs from any other ordinary and continuous writing and does not contain data that is arranged in a way that is individually accessible. The court thus required some “technical access key”, however simple, such as a table of contents or an index, that gives access to the individual data of the collection, in order for a collection of data to be considered a protectable database. (Court of Appeal Brussels 5 June 2007).

UPCOMING LEGISLATIVE CHANGES

None at a national level (see [EU section](#)).

TOP TIP FOR THOSE LOOKING TO EXPLOIT BIG DATA

Manage your big data in view of both the data’s value to your organization and the data’s degree of toxicity: valuable data is data that is of commercial, financial or strategic importance to the organisation, whereas toxic data is data to which third parties’ personal, intellectual property or other rights are attached, such as personal data, product designs, copyrighted works etc. Both categories of data do not necessarily coincide but do have in common that they could be damaging to your organisation if they left your organisation’s control. Therefore, it is advisable to prepare a big data policy with different protection and security scenarios and mechanisms depending on whether the stored and processed data may contain valuable or toxic data or not.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

4. BRAZIL

KEY CONTACTS



Antonio Murta Filho
Founding Partner
T +55 21 3553 6575
antonio.murta@
murtagoyanes.com.br



Marcelo Goyanes
Founding Partner
T +55 21 3553 6575
marcelo.goyanes@
murtagoyanes.com.br

ORIGINAL DATABASE

Protected? The information structure of databases is protected in Brazil by Copyright Law (the data contained therein may be protected by Unfair Competition Law and Criminal Law).

Ownership Usually, the copyright owner is the author of the work. However, if the database was created as a collective work, organized by and under the instructions of a third party, the latter will retain ownership over it, but must still observe the moral rights of each contributor. Rights over a database may also be assigned.

Pre-conditions The information structure of the database must constitute an intellectual creation.

May cover Copyright protection applies to all kinds of databases, regardless of the data contained therein.

Duration Copyright protection endures for 70 years after the end of the calendar year in which the author (or the last author, if the database is a work of joint authorship) dies.

Scope of Protection Copyright Law does not protect the information contained in the databases, only the arrangement of the data (art. 7º, §2º, Law 9.610/98). Nevertheless, database owners may authorize or prohibit:

- its full or partial reproduction, by any means or process;
- its translation, adaptation, rearrangement or any other modification;
- reproduction, distribution or communication to the public of the results of the operations referred to in item II; and
- distribution of the original or copies of the database, as well as its communication to the public.

Remedies include: Injunctions, damages and loss of profits.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Databases in which investments have been made do not have any separate protection in Brazil beyond the protections described elsewhere in this chapter on Brazil.

CONFIDENTIAL DATABASES

Notwithstanding the copyright protection granted to the information structure of a database, the data contained therein may be specially protected as Trade Secrets by Unfair Competition Law and Criminal Law.

Pre-conditions: The information contained in the database will not be considered confidential information, unless: (i) the information is not generally known and it may not be easily accessible; (ii) the protected information has economic value; and (iii) the owner has taken significant measures to ensure the confidentiality of the information.

May cover: Clients lists, manufacture processes, advertising strategies, etc.

Unlikely to cover: Information publicly known or without economic value.

Duration: Protection arises from the moment the information is created and endures as long as the information contained in the database remains confidential.

PERSONAL DATA

Is personal data given particular protection? Brazil does not have a law that is specifically devoted to personal data protection. However, on April 23rd, 2014, Brazil's President sanctioned Federal Law 12.965/2014, also called the Internet Civil Rights Framework and the "Brazilian Internet Constitution". This law establishes principles, rights and obligations for the use of the Internet in Brazil and has several provisions concerning the storage, use and disclosure of data collected through the Internet.

Moreover, there are general principles and provisions on data protection and privacy in the Federal Constitution, the Civil Code and in laws and regulations that address particular types of relationships (e.g. the Consumer Protection Code⁴ and labour laws), particular sectors (e.g. financial institutions, health industry, telecommunications etc.), and particular professional activities (e.g. medicine and law).

Who can rely on it? The individuals that are the subject of the data, as well as several consumer protection bodies.

What data? Although there is not a definition of "Personal data", it could be interpreted as a person's financial, health, educational records and contact information.

⁴ Due to a broad interpretation established in case law, practically every internet user is considered a 'consumer' for the purposes of the consumer protection.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

Since April 2013, it is also possible to criminally prosecute the persons responsible for hacking into any digital device used to store data which has been collected. More severe penalties may be imposed if: (i) the information illegally obtained is confidential; (ii) the information illegally obtained is divulged, traded or transmitted to third parties; or (iii) the hacking provokes economic harm to the data owner.

Additionally, there are laws on the treatment and safeguarding of documents and information handled by governmental entities and bodies that have privacy implications.

SIGNIFICANT RECENT CASES

Curriculum Tecnologia Ltda. vs. Catho On Line S/C Ltda.: This case involved two competing companies that specialized in helping companies hire professional personnel by advertising résumés and job openings online. Curriculum Tecnologia's users posted their résumés online upon payment of a monthly fee, and companies would browse the résumés for potential candidates.

In 2002, Curriculum Tecnologia filed a lawsuit claiming that Catho was practising unfair competition by using programs to illegally obtain (through data scraping) copies of thousands of résumés from its database. In 2011, the first level judge recognized the practice of unfair competition and condemned Catho to pay damages of approximately US\$ 32,360,000.00.

The parties settled in 2013 without disclosing the amount of the settlement.

UPCOMING LEGISLATIVE CHANGES

The Senate proposed Bill of Law 330/2013 to establish principles, rights and obligations for the use and treatment of personal data in Brazil, as well as its transmission abroad. This bill is pending discussion by the Senate's committees and the Plenary and, once approved, it will be sent to the House of Representatives. The Ministry of Justice is supposedly also working on a draft for a Data Protection bill of law to be presented to Congress.

TOP TIP FOR DATABASE OWNERS

Keep public records of the information structure of the database and private records of the information contained therein.

TOP TIP FOR THOSE LOOKING TO EXPLOIT BIG DATA

Audit your data: Brazilian Law may protect the information you process.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

5. CHINA (PEOPLE'S REPUBLIC OF CHINA)

KEY CONTACTS



Richard Wageman
Partner
T +8610 6561 1788
richard.wageman@dlapiper.com

ORIGINAL DATABASES

Protected? Original databases are protected by Copyright Law of the People's Republic of China as a "compiled work" or works created through compiling works, segments of works or data or other materials not constituting a work, provided that there is sufficient originality in selection or arrangement of the compiled work. (Article 14 of the Copyright Law).

Ownership Copyright in the database vests with the compiler or author of the database. However, the compiler shall not infringe copyright in the original work when exercising his or her copyright as a compiler.

Pre-conditions The database must be "original", particularly for the selection or arrangement. Copyright does not need to be registered to be protected. However the PRC does have an optional procedure to register copyright, which is helpful when trying to prove ownership.

May cover Marketing databases with more complex structures based on assessments of customer or business needs.

Unlikely to cover Databases which are produced by an automated computer process.

Duration Excluding the right of authorship, right to alteration and right to have work integrity protected which are protected infinitely in duration, copyright protection in the PRC lasts for the duration of the author's life plus 50 years after his or her death (this applies to the last author for instances of joint authorship).

Scope of protection Subject to the limitation on rights provided under Articles 22 and 23 of the Copyright Law, database owners may prevent third parties from making the database (or copies) available to the public and can also prevent third parties from conducting acts that are either without authorization or outside the scope of copyright licenses (such as the altering, adapting, translating, copying or hiring out the database).



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Remedies: Infringement of copyright may result in:

- **Civil Liability and Remedies.** Examples include requirement on the infringer to stop the infringing acts, to take steps to eliminate the harm caused, apologising or paying compensation for losses (Article 47 of the Copyright Law). Where the copyright owner has evidence that others are conducting or are about to perform acts that may infringe his or her copyright which may result in irreparable harm to his or her legal rights if such act is not stopped in time, the copyright owner may apply to the People's Court before litigation for an order to stop the relevant acts or a measure to take property as security (Article 50 of the Copyright Law);
- **Administrative Sanctions.** Where public interest has been harmed, in addition to any applicable civil liability or remedies, the copyright administrative agencies may order 1) administrative injunction against the infringing acts; 2) confiscation of illegal earnings; 3) confiscation or destruction of infringing products; or 4) fines. Where the breach is serious, the copyright administrative agencies may also confiscate materials, tools and equipment used to produce the copyright infringing product (Article 48 of the Copyright Law); and
- **Criminal Liability:** See Article 48 of the Copyright Law and Article 214 of the Criminal Law the People's Republic of China (2011 Revision; **Criminal Law**).

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Databases that involve investment in their compilation do not have any separate protection in the PRC.

CONFIDENTIAL DATABASES

Protected? In addition to the copyright protection, confidential databases may be protected as commercial secrets under the **Anti-Unfair Competition Law** of the People's Republic of China (link is to an English version; **Anti-Unfair Competition Law**) and the Criminal Law, provided that such database is valuable for the company and has been kept confidential (Article 10 of the Anti-Unfair Competition Law).

Owner Anti-Unfair Competition Law and Criminal Law protect the rights of database owners.

Pre-conditions Involves the efforts of the owner/author to keep it confidential.

May cover Anti-Unfair Competition Law and the Criminal Law cover databases containing information which is largely unknown outside the owner's business.

Unlikely to cover Databases consisting of readily available information and databases that are not difficult for others to duplicate.

Duration Protection arises from when the database (which the owner has made efforts to keep confidential) is created and will last until publication by the owner or an authorised party.

Scope of protection Unauthorised acts include unauthorised publishing or use of the confidential database.

Remedies Owner of the database may recover compensation for loss suffered from a breach and may obtain injunctions to prevent intended infringement, where it has yet to occur. Infringers may also be subject to criminal sanctions, if applicable.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

PERSONAL DATA

Is personal data given particular protection? The PRC does not have comprehensive personal data protection law but there are general requirements to protect personal data in the General Principles of the Civil Law of the People's Republic of China (**GPCL**), the Criminal Law of the People's Republic of China (**Criminal Law**) and the Tort Liability Law of the People's Republic of China (**Tort Law**). The three laws above are all national laws.

In addition to the above national laws, personal data is also protected under the Decision of the Standing Committee of National People's Congress in Strengthening Internet Information Protection (**Decision**) and the Consumer Rights and Interested Protection Law of the People's Republic of China (**Consumer Rights Law**).

Compliance with the Guidelines for Personal Information Protection within Information System for Public and Commercial Services (GB/Z 28828-2012; the **Guidelines**), which is a non-binding national standard, is recommended as the better practice approach.

Who can rely on it? Individuals to whom the information relates may rely on the protection.

What data? GPCL, Criminal Law and Tort Law are very general on the protection and we understand such protection applies to all data about individuals. The Decision protects electronic information that may identify a citizen's personal identity or those that may relate to personal privacy. The Consumer Rights Law applies to consumers' personal information. The Guidelines applies to computer data that: 1) can be processed by an information system; 2) relates to certain natural persons; and 3) can be used either independently or jointly with other information to identify the natural person.

Scope of protection The scope of these laws varies:

- GPCL protects reputation rights, breach of which has been interpreted by the Supreme People's Court of China to include the disclosure of personal privacy that results in certain influences;
- Criminal Law prohibits the illegal provision or sale of a citizen's personal information acquired during business activities by institutions in certain industries (e.g. telecom and financial industries);
- Tort Law prohibits unauthorized disclosure of a patient's medical records by a medical institution or its staff;
- The Decision and Consumer Rights Law largely require the same: 1) notification and consent on the scope, purpose, method and rules of any data collection and use; 2) data confidentiality; 3) secured protection of personal data collected; and 4) prohibition on sending commercial information to the data subject where there has not been a consent or request, or where there has been a stated refusal; and
- The Guideline recommends rules that may be followed when a business is collecting, processing, storing, transferring or deleting personal information.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

The following types of data are subject to particular protection:

- Personal data obtained by financial institutions (banks) is subject to more strict rules, requiring them to protect their clients' financial data;
- Personal data collected during online transactions is specifically protected under the Administrative Measures for Online Trading issued by the State Administration for Industry and Commerce (**Measures**). The Measures' requirements for protection of consumer's personal information are similar to those established under the Guidelines.
- Telecom and Internet information service providers are subject to the Provisions on the Protection of Telecommunication and Internet User Personal Information (**Provisions**). For the purposes of the Provisions, businesses that collect personal data from the Internet are recommended to comply as an Internet information service providers; and
- Information and data regarded as containing state secrets are subject to strict requirements on data monitoring, access, use and transfer as provided under the laws and regulations relating to state secrets (though what is a state secret is defined very broadly under the PRC legal regime, we understand the definition to apply mostly in rare circumstances and sensitive industries).

SIGNIFICANT RECENT CASES

Most cases are not publicly available. The PRC legal regime is not based on case law precedents.

UPCOMING LEGISLATIVE CHANGES

The Chinese government is in the process of preparing comprehensive data privacy legislation. It is not yet known when this will be enacted.

TOP TIP FOR DATABASE OWNERS

Protection of databases in the PRC is assisted by keeping records which identify the authors of the information in the database.

TOP TIP FOR THOSE WHO EXPLOIT BIG DATA

Where data is collected from a third party data provider, businesses should contractually require the third party data provider to be responsible for ensuring that the data is acquired and provided legally. Where data is collected by the businesses themselves, businesses should be aware of the types of data being collected, since some of these data may be sensitive data that would require additional legal compliance. For instance:

- If personal data is collected, any such collection and use should be notified and consented to by the data subjects (i.e. employees and customers); or
- If data collected is regarded or is likely to be regarded as state secret, any access, use and transfer of such data should be restricted and monitored accordingly.



- Australia
- Austria
- Belgium
- Brazil
- China
- EU**
- France
- Germany
- Hong Kong
- India
- Italy
- Japan
- The Netherlands
- Romania
- Singapore
- South Africa
- South Korea
- Spain
- Turkey
- UK
- USA

6. EU

EU law in this area is only partly harmonised; to the extent that there is national variation, this is dealt with in the national sections covering the representative EU jurisdictions *France, Germany, The Netherlands, Spain and the UK*.

KEY CONTACTS

Austria

Sabine Fehringer

Belgium

Patrick van Eecke

Alexis Fierens

France

Sandrine Rambaud

Stephane Lemarchand

Germany

Jan Pohle

Christopher Goetz

Hungary

Zoltan Kozma

Italy

Roberto Valenti

Stefania Baldazzi

Netherlands

Robin de Wit

Alexander Tsoutsanis

Niels Mulder

Spain

Diego Ramos

UK

John Wilks

Jim McDonnell

ORIGINAL DATABASES

Protected? Databases are protected by copyright as a database, “Database” is defined as “a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means” under the [EU Database Directive 96/9](#).

Ownership. The protection is given to the database author(s) or creator(s).

Pre-conditions A database must satisfy the definition above and “constitute the author’s own intellectual creation” by reason of the “selection or arrangement” of the database’s content. The author’s own intellectual creation requirement has been expressed as the author expressing “his creative ability in an original manner by making free and creative choices” and stamp a “personal touch”⁵. There is no requirement for copyright in the database to be registered.

⁵ *Football Dataco v Yahoo*, see below.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

May cover Marketing databases with a complex structure, an anthology of poems structured by theme.

Unlikely to cover Telephone directories, record of live actions occurring during a sporting event.

Duration Protection in the database applies automatically once the database exists in material form and will last for 70 years after the end of the calendar year in which the author died.

Scope of protection Infringement will arise by temporarily or permanently reproducing the database, translating, adapting or altering the database or distribution or communication to the public of copies of it without authorisation of the owner.

Remedies EU remedies include injunctions (both interim and final) and the recall or destruction of infringing materials or materials used to create infringing copies, damages and payment of legal costs⁶.

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Protected? Databases that involve investment are also protected as the definition of database under the Database Directive is the same as for copyright.

Ownership The maker of the database (the person who “takes the initiative and the risk of investing”) is protected; however, if the work is subcontracted it will be the commissioner of the sub-contract⁷.

Pre-conditions Investment in “obtaining” must not have been in the creation of the data which is the subject of the database, but rather in seeking out existing independent materials and collecting them in the database⁸. The maker or rightholder of the database (where a company or firm) must have its registered office, central administration or principal place of business within the EU.

May cover Marketing databases, a record of live actions occurring during a sporting event, case law databases, databases of rainfall in particular locations, database of contact details for people working in doctors’ surgeries, collection of car advertisements hosted on a website.

Unlikely to cover A list of runners and riders in a horse race.

Duration The right arises on creation of the database and lasts 15 years from its creation or (if later) it being made available to the public. A new 15 year period right is commenced when substantial updates or changes are made to the database.

⁶ EU IP Enforcement Directive 2004/48

⁷ Recital 41 of the Database Directive.

⁸ This results from CJEU case law, including in particular *British Horseracing Board v William Hill C-203/02*



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Scope of protection The right can prevent:

- Extraction or reutilisation of the whole or a substantial part (evaluated by qualitative and/or quantitative analysis) of the contents of the database and
- Repeated and systematic extraction or re-utilisation of insubstantial parts of the contents of the database

Remedies The remedies for infringement are broadly the same as for copyright, as above.

CONFIDENTIAL DATABASES

There is currently no EU wide law protecting confidential information – this is covered by national law⁹.

PERSONAL DATA

Is personal data given particular protection? Handling personal data is subject to the [EU Data Protection Directive 95/46](#), which has been implemented by national legislation across the EU.

Who can rely on it? Individuals who are the subject of the personal data (“**data subjects**”) are protected by the Directive. Data subjects have various rights, including the right to be informed when their data is being processed.

What data? “Personal Data” is a wide definition which includes any information relating to an identified or identifiable natural person. It can include contact information such as e-mail addresses and telephone numbers, financial information and health information.

Scope of protection The legislation regulates the processing of personal information, mainly through imposing obligations on data controllers. This can limit what the owner of a database can legitimately do with that database (particularly marketing databases).

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

In general terms there are no other types of protection for data or databases.

SIGNIFICANT RECENT CASES

Football Dataco v Yahoo: Court of Justice of the European Union ruled in a case dealing with football match schedules that the criterion of “author’s own intellectual creation” for database copyright:

- (i) requires that the author express his creative ability in an original manner by making creative choices and
- (ii) is not satisfied when the setting up of the database is dictated by technical constraints which leave no room for creative freedom

⁹ The EU has commissioned a [comparative study of the protection of trade secrets across the EU](#); see also “Upcoming Legislative Changes” section below.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Football Dataco v Sportradar: CJEU held (in a case involving a database of data gathered live during football matches) that a database owner can sue an online infringer of database right where internet users whom the infringer intends to target are located.

Autotrack v Gaspedaal.nl: see description in the Netherlands section.

Directmedia v Albert-Ludwigs-Universitaet: the CJEU explained that the “extraction” act of infringement in relation to database right:

(i) should be given a wide definition; and

(ii) would include transfer of material from a protected database to another database following an on screen consultation of the first database and an individual assessment of the material contained in it.

This case involved an anthology of poems, which was used to produce a CD-Rom of a collection of poems.

Google v Agencia Española de Protección de Datos: the CJEU confirmed that a data subject can require Google to remove him/her from search results. This potentially opens the door to a similar “right to be forgotten” being enforceable against controllers of databases more generally (especially publicly accessible ones). The decision also means controllers of personal data hosted outside the EU by a non-EU company are likely to have to comply with EU data protection law where they have EU subsidiaries which undertake activities which are closely linked to the controller’s data processing activities.

UPCOMING LEGISLATIVE CHANGES

The European Commission (“**Commission**”) introduced a Public Consultation on the Review of EU Copyright Rules in December 2013, which closed on 5 March 2014. One of the areas covered was whether copyright causes a barrier to text and data mining. The Commission is still currently analysing the responses and has indicated that it will publish a summary of the responses in 2014.¹⁰

Draft legislation will follow the analysis of the responses, and it is possible that we will see a new EU-wide defence covering this use at some point in the next few years. However, the legislation covers a large number of other controversial topics, so progress of this is likely to be fairly slow.

On 28 November 2013 the European Commission published a proposed Directive on the protection of trade secrets against their unlawful acquisition, use and disclosure¹¹ (“**Trade Secrets Proposal**”). This would generally improve the position for database owners in giving a more harmonised form of protection to this currently unharmonised area, and making it

¹⁰ http://ec.europa.eu/internal_market/consultations/2013/copyright-rules/index_en.htm

¹¹ The text of the proposal is [here](#) and the Compromise text can be found within the Council opinion at <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209870%202014%20INIT>



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

easier for national courts to deal with the misappropriation of confidential business information. The Trade Secrets Proposal has only recently been published and parliamentary work on it is unlikely to begin until Autumn 2014. However, on 4 March 2014, in response to comments received on the Trade Secrets Proposal, the Council published a presidency compromise proposal which amended the first draft. On 26 May 2014, the Council rendered its opinion on the draft proposal¹². The Council will now start negotiations with the European Parliament, whose response should be available within 2014.

A new Data Protection Regulation is currently being negotiated, which will impose significantly more extensive obligations on data controllers. To become law the proposed Data Protection Regulation has to be adopted by the Council of Ministers using the co-decision procedure. The Parliament stands ready to negotiate with the Council of the EU (“**Council**”) as soon as the Council defines its position.

For information on latest status, consult the DLA Piper [Privacy Matters blog](#).

TOP TIP FOR DATABASE OWNERS

In the EU, to obtain database right documenting the investments and structure underlying your database is as important as building the database itself. How the information is obtained/verified/presented and how much you have invested in each of these processes, is critical to obtain and invoke protection. Lack of such evidence is often a cause for delay or difficulty in enforcing your rights in the database later on.

TOP TIP FOR THOSE WHO EXPLOIT BIG DATA

Consider locating data-gathering companies in the EU, so as to qualify for an EU database right (though if the data is personal data there may be a trade-off with the inconvenience of this potentially leading to greater obligations under EU data protection law). Also look ahead to the new Data Protection Regulation, and seek to ensure your databases and processes for gathering, processing and exploiting big data are designed to ensure compliance.

¹² The Council Press release can be found at: http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/intm/142780.pdf



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

7. FRANCE

KEY CONTACTS



Stephane Lemarchand
Partner
T +33 | 40 15 24 46
stephane.lemarchand@
dlapiper.com



Jeanne Dautier
Associate
T +33 | 40 15 24 17
jeanne.dautier@dlapiper.com

The law is part harmonised with general EU law (see [EU section](#)). In this section we therefore only highlight areas that differ from EU-wide law.

ORIGINAL DATABASES

Protected? The EU-wide Database Directive is implemented in France by Article L. 112 3 of the [French Intellectual Property Code \(FIPC\)](#); link is to French language version).

Pre-conditions In addition to the requirements under EU law, the arrangement of the data should not result from a simple compilation, but rather should result from free choices and constitute the author's own intellectual creation *SA les Editions du Boisbaudry v. SA le Pont Veterinaire*¹³. There is no requirement for copyright notices or registration.

Scope of protection The infringing acts are set out in Article L.335-2 and seq. of the FIPC (See [EU law section](#))

Remedies Article 1-331-I onwards of the FIPC provides for:

- Injunctions (interim and final)
- Recall/destruction of infringing materials/materials used to create infringing copies
- Damages
- Payment of legal costs

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

The Database Directive is implemented by articles L.341-1 and seq. of the FIPC (please see [EU section](#)).

¹³ September 2004 03/04746



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

CONFIDENTIAL DATABASES

There is no right to prevent misappropriation/misuse of confidential information, other than via contractual obligations, under non-disclosure agreements.

PERSONAL DATA

See [EU section](#). The handling of “personal data” is subject to the [EU Data Protection Directive 95/46](#), which has been implemented in France by the Law of 6 January 1978 as amended ([English version here](#)).

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

Generally no, however access to public data is governed by special legislation.

SIGNIFICANT RECENT CASES

Precom and Ouest France v. Direct Annonce: the French Supreme Court refused the protection of sui generis database right to a database of real estate advertisements included in the different versions of a newspaper, because the investment was not related to obtaining the contents of the database but to the creation of the items included in this database and the purely formal verification operations, during this creation phase.

Pressimmo online v. Yakaz and Gloobot: The Court of Appeal of Paris refused the protection of sui generis database right to a website of real estate advertisements, because the website owner only alleged having made substantial investments and did not break down the investments (obtaining, verification and presentation) and did not prove the substantiality of such investments. Moreover, the Court stated that the website owner could use the unfair competition regime to bypass the sui generis database right.

UPCOMING LEGISLATIVE CHANGES

None at a national level (see [EU section](#)).

TOP TIP FOR DATABASE OWNERS

Include “seeds” (deliberately inserted fake information) in your database, so that you can trace and prove infringement.

TOP TIP FOR THOSE WHO EXPLOIT BIG DATA

Ensure that the data have been collected lawfully, and in particular in accordance with French data protection law.



- Australia
- Austria
- Belgium
- Brazil
- China
- EU
- France
- Germany**
- Hong Kong
- India
- Italy
- Japan
- The Netherlands
- Romania
- Singapore
- South Africa
- South Korea
- Spain
- Turkey
- UK
- USA

8. GERMANY

KEY CONTACTS



Jan Pohle
Partner
T +49 221 277 277 390
jan.pohle@dlapiper.com



Christopher Goetz
Senior Associate
T +49 221 277 277 392
christopher.goetz@dlapiper.com

The law is part harmonised with general EU law (see [EU section](#)). In this section we therefore only highlight areas that differ from EU wide law.

ORIGINAL DATABASES

Protected? Databases are protected by copyright as a “database”. Subject to the EU-wide [EU-Database Directive 96/9](#) (see [EU section](#)), implemented by the *Urheberrechtsgesetz* (German Copyright Act) — “**UrhG**”, link is to the English translation Section 4 para. 2 of which defines “database”.

Section 4 UrhG in its present form was implemented by Article 7 of the German Information and Communication Services Act of 1997.

Pre-conditions The “*author’s own intellectual creation*” is required (“*persönliche geistige Schöpfung*”) and is implemented by Section 2 para. 2 UrhG, and Section 4 para. 1 UrhG.

Remedies In instances of intentional infringement there are potential criminal sanctions, including imprisonment of up to three years or a fine (Section 106 UrhG). If intentional infringement is on a commercial basis (“*gewerbsmäßig*”), the sanctions can be imprisonment of up to five years or a fine (Section 108a UrhG).

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Protected? Some databases may be subject to the EU-wide [EU-Database Directive 96/9](#) (see [EU section](#)), implemented in Germany by Section 87a — 87e UrhG. These Sections were implemented by Article 7 of the German Information and Communication Services Act of 1997.

Scope of protection Section 87b para 1 Sentence 2 UrhG states that the repeated and systematic extraction or re-utilisation of insubstantial parts of the contents of the database can only be prevented by the rights holder if such acts do not amount to a “normal use” of the database or if such acts cause undue prejudice to the legitimate interests of the maker of the database.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

CONFIDENTIAL DATABASES

Protected? It is possible for confidential databases to be protected, under legal provisions that protect confidential information. In particular, Section 17 of the German [Unfair Competition Act](#) (Gesetz gegen den unlauteren Wettbewerb — “**UWG**”, link is to the English translation) renders it a criminal offence to disclose, acquire or secure, without authorisation, trade and industrial secrets. There is no parallel civil right of action for those whose confidential information is taken, unless they are able to sue for breach of contract under an NDA.

Ownership The law in this area protects the owner of the business to which the trade and industrial secrets belong.

Pre-conditions Protection will in particular arise where there are “unauthorised communications”, which include:

1. communication of trade or industrial secret (facts, circumstances and procedures, which are not obvious, and only accessible to a limited circle of persons and with regard to which the right holder has a legitimate interest not to make them public)
2. by an employee of a business, who was entrusted with or who had access to such trade or industrial secret during the course of the employment relationship and
3. for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business (Section 17 para. 1 UWG)

May cover Customer databases, databases of a company’s commercial or technical knowhow, databases of product ingredients.

Unlikely to cover Data which is published or licensed on terms which do not impose confidentiality obligations.

Duration The protection arises from the time the obligation of confidentiality arises, and will last until the obligation ceases (e.g. usually until the information passes into the public domain).

Remedies Potential remedies in this area involve criminal sanctions (either imprisonment or fines). Industrial espionage by employees or others (Section 17 para.2 number 1 UWG), and unauthorised exploitation of trade and industrial secrets (Section 17 para number 2 UWG) can also give rise to criminal liability.

PERSONAL DATA

The handling of “personal data” is subject to the Federal Data Protection Act ([Bundesdatenschutzgesetz](#) – “**BDSG**”; link is to English translation).

The EU Data Protection Directive has been implemented into the BDSG by the German Act to Modify the BDSG, dated May 18, 2001. Additional data protection provisions are provided in legislation such as the German Telecommunication Act (Telekommunikationsgesetz – “**TKG**”) and the German Telemedia Act (Telemediengesetz – “**TMG**”).



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Failure to comply with data protection law is aggressively prosecuted in Germany. Infringements may lead to the imposition of severe (criminal and administrative) fines and even imprisonment. (See [EU section](#)).

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

Generally, no. With regard to personal data collected by the state and other public bodies, there are specific provisions within the BDSG.

SIGNIFICANT RECENT CASES

“Automobil-Onlinebörse” (I ZR 159/10): The German Federal Court of Justice (Bundesgerichtshof – “BGH”) held that a meta-search engine, which enables individual users to conduct specific searches of protected databases, (in the case at hand an online automobile-market), does not infringe the database maker’s exclusive right to “distribute and reproduce its database”, since:

- the meta-search engine does not reproduce a substantial part of the database (single queries only) and
- the repeated use of insubstantial parts of the database does “not amount to an illegitimate reproduction of a substantial part” (meta-search engine does not intend to create a copy of the full/substantial part of the database).

Please note: This BGH decision of 2011 stands in stark contrast to the recent decision of the CJEU concerning the interpretation of Art. 7 of the Database Directive in matters [Innoweb vs. Wegener](#). In its decision the CJEU held that a dedicated meta search engine may very well “re-utilise the whole or a substantial part of the contents of a protected database” – and therefore may infringe the rights of a database maker – where the dedicated meta search engine:

- provides the end user with a search form which essentially offers the same range of functionality as the search form on the database site;
- ‘translates’ queries from end users into the search engine for the database site ‘in real time’, so that all the information on that database is searched through; and
- presents the results to the end user using the format of its website, grouping duplications together into a single block item but in an order that reflects criteria comparable to those used by the search engine of the database site concerned for presenting results.

The CJEU decision will most likely have an impact on any future judgments of the BGH concerning this so-called ‘screen scraping’.

UPCOMING LEGISLATIVE CHANGES

A new [European-wide Data Protection Regulation](#) is currently being drafted (see [EU section](#)), which is expected to modify the current German data protection law. On 30 March 2012 the German Federal Assembly (*Bundesrat*) issued a formal complaint (*Subsidiaritätsrüge*) on this



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

new regulation since — in the Bundesrat’s view — the regulation does not comply with Art. 5 Para. 3 of the Treaty on European Union. The prevailing opinion in German legal literature and with legal scholars is that the complaint of the Bundesrat will not be successful¹⁴.

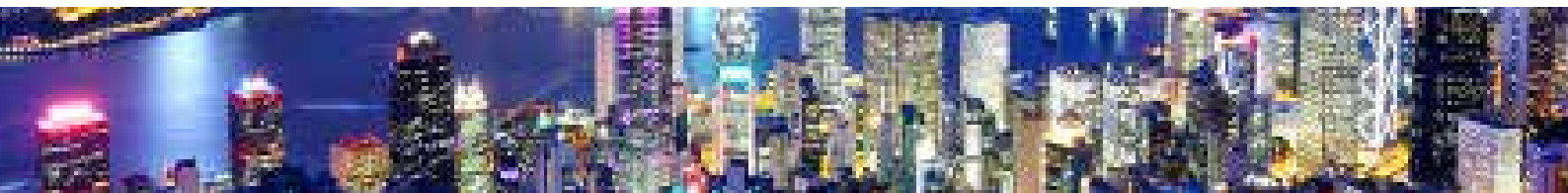
TOP TIP FOR DATABASE OWNERS

Audit the data you collect, process or use: ensure that you obtain all necessary rights to exploit such data. If the data contains “personal data”, ensure that you are compliant with the BDSG (e.g. by obtaining the consent of the data subjects to process or use their personal data).

TOP TIP FOR THOSE WHO EXPLOIT BIG DATA

Big data projects bring with them not only significant concerns with regard to data protection/privacy, but also with regard to third parties’ IP infringements. Ensure compliance with applicable data protection laws and keep track of the sources from which data is legitimately collected in order to be able to defend any infringement claims.

¹⁴ Nguyen, „Die Subsidiaritätsrüge des Deutschen Bundesrates gegen den Vorschlag der EU-Kommission für eine Datenschutzgrundverordnung“, ZEuS, 2012, p. 277 – 300; [Statement of Prof. Boehm of Westfälische Wilhelms – University dated 26 Februar 2013](#)



- Australia
- Austria
- Belgium
- Brazil
- China
- EU
- France
- Germany
- Hong Kong
- India
- Italy
- Japan
- The Netherlands
- Romania
- Singapore
- South Africa
- South Korea
- Spain
- Turkey
- UK
- USA

9. HONG KONG

KEY CONTACTS



Scott Thiel
 Foreign Legal Consultant
 T +852 2103 0519
 scott.thiel@dlapiper.com



Edward Chatterton
 Foreign Legal Consultant
 T +852 2103 0504
 edward.chatterton@dlapiper.com

ORIGINAL DATABASES

Protected? Original databases are protected by copyright as a ‘literary work’, which includes compilations of data or other material, in any form which, by reason of the selection or arrangement of their contents constitutes an intellectual creation¹⁵. Such compilations of data may be expressed in writing or otherwise and are protected by copyright regardless of the method or the medium in or on which they are recorded¹⁶. The relevant legislation in this area is the **CAP 528 Copyright Ordinance**.

Ownership Generally the author of a work is the first owner of any copyright, unless the work is created by an employee in the course of his employment (in which case the employer is the first owner, subject to any agreement to the contrary)¹⁷. If the database is computer-generated, the author is taken to be the person by whom the necessary arrangements for the creation of the work are undertaken.

Pre-conditions In order for a database to be protected, the following requirements must be met:

- the database must be “original” in that it must not have been copied from another and must have originated from an author¹⁸;
- the author must have put in a sufficient level of skill, judgement and labour in the making of the database¹⁹; and
- the database must have been reduced to material form (e.g. recorded, in writing or otherwise)²⁰. Note that copyright protects the expression of ideas, not the ideas themselves. In the case of a database, if copyright arises, it is the selection or arrangement of data that is protected not the underlying data itself.

¹⁵ Section 4 of the Copyright Ordinance

¹⁶ Section 198(1) of the Copyright Ordinance

¹⁷ Sections 11, 13 and 14 of the Copyright Ordinance

¹⁸ *University of London Press Ltd v University Tutorial Press Ltd* [1916] 2 Ch at 608-609

¹⁹ *Greyhound Racing Association Ltd v Shallis* [1923-28] MCC 370 at 373, per Eve J.

²⁰ Section 4 of the Copyright Ordinance



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

May cover Marketing databases with more complex structures based on assessments of customer or business needs.

Unlikely to cover Databases which are, to a significant degree, produced by an automated computer process and the making of which involves little or no skill, judgement and labour.

Duration Copyright is an automatic right which arises when a work is created. It is not necessary to register copyright in Hong Kong in order to qualify for protection. There is no official registry in Hong Kong for registration of copyright works. Protection generally lasts for the life of the author(s) and for 50 years after the end of the calendar year in which the author (or the last author, if the database is a work of joint authorship) dies. If the database is computer-generated, copyright expires at the end of 50 years from the end of the calendar year in which the database was made.

Scope of protection Copyright protection gives the owner the exclusive rights, most relevantly, to do the following acts in Hong Kong:

- Copy the database;
- Issue/rent copies of the database to the public;
- Make copies of the database available to the public; and
- Make an adaptation of the database or do any of the above in relation to an adaptation.

Copyright is infringed by a person who, without the license of the copyright owner, does or authorises another to do any of the acts above in relation to a database as a whole, or any substantial part of it, either directly or indirectly.

Remedies A copyright owner may take civil legal action against any person who infringes copyright in the work. The owner may seek all necessary relief against the infringer, including injunctions to prevent further infringement, an order for delivery up of the infringing items, disclosure of information about the supply and/or dealings of the infringing items and an award for damages, accounts of profits as well as costs.

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Databases in which investments have been made do not receive protection beyond the other protections discussed above and below.

CONFIDENTIAL DATABASES

Protected? It is possible for confidential databases to be protected under the law of confidence, arising from contract (expressed or implied) or under the common law of confidence. The right to restrain a breach of confidential relations is preserved by the Copyright Ordinance.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

See the case law in the UK section below (**Coco v AN Clark (Engineers) Ltd**) which applies to Hong Kong. Unlike other Commonwealth common law jurisdictions, which treat confidentiality and trade secrets as equitable rights, in Hong Kong it has been held that confidential information can be property. The threshold for breach of confidentiality depends on the circumstances of the case (e.g. employment²¹).

Owner The owner of the database is the person protected, but only in circumstances where the recipient owes the owner an obligation to keep the information confidential (i.e. if a reasonable person in the position of the recipient would understand that the information was given in confidence).

Pre-conditions The information contained in the database will not be protected under the law of confidential information unless:

- (i) the information has the necessary quality of confidence;
- (ii) the owner has taken sufficient steps to preserve the confidentiality of its information; and
- (iii) a reasonable person in the position of the recipient would understand that the information was given in confidence.

May cover Databases containing information which is largely unknown outside the owner's business.

Unlikely to cover Databases which consist of readily available information or are not difficult for others to duplicate or databases which are licensed on terms which do not impose obligations of confidentiality.

Duration Protection arises from the time the obligation of confidence arises (provision of the confidential database), and lasts until the obligation ceases (until the information passes into the public domain).

Scope of protection In addition to the items listed above it is necessary to establish that

- (i) the information was imparted in circumstances importing an obligation of confidence; and
- (ii) there has been an unauthorised use (or threatened unauthorised use) of that information to the detriment of the party communicating it.

Remedies

- Injunctions (interim and final)
- Damages or an account of profits
- Delivery up or destruction
- Payment of legal costs

A claimant may be required to elect whether to claim damages for breach of confidence or for infringement of copyright.

²¹ See *Faccenda Chicken Ltd v Fowler* [1987] Ch.117



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

PERSONAL DATA

Is personal data given particular protection? The **Personal Data (Privacy) Ordinance Cap. 486** (“**PDPO**”) covers the law in this area.

Who can rely on it? The individual who is the subject of the personal information may rely on the law.

What data? Any data that relates directly or indirectly to a living individual (the “**data subject**”), from which it is reasonably practicable to ascertain the identity of the individual and which is in a form in which access or processing is practicable (“**Personal Data**”).

Scope of protection The Privacy Commissioner of Personal Data regulates the control, collection, holding, processing and use of Personal Data. Use and provision of Personal Data in direct marketing is heavily regulated and there are limits on what the owners of a database can legitimately do with that database (particularly a marketing database).

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

No.

SIGNIFICANT RECENT CASES

There have not been any significant recent cases in respect of rights in data/databases in Hong Kong.

UPCOMING LEGISLATIVE CHANGES

Section 33 of the PDPO, which provides a stringent and comprehensive regulation of cross-border transfer of Personal Data outside Hong Kong, is expected to be implemented in the near future. This section expressly prohibits all transfers of Personal Data outside Hong Kong unless one of the exemptions applies. Accordingly, to the extent that databases are located outside Hong Kong, those data users who transfer Personal Data to such databases are expected to have to comply with this section once it is implemented.

TOP TIP FOR DATABASE OWNERS

Protection of databases is assisted by ensuring that adequate contractual protections are in place/accepted prior to or at the time of accessing the database, including:

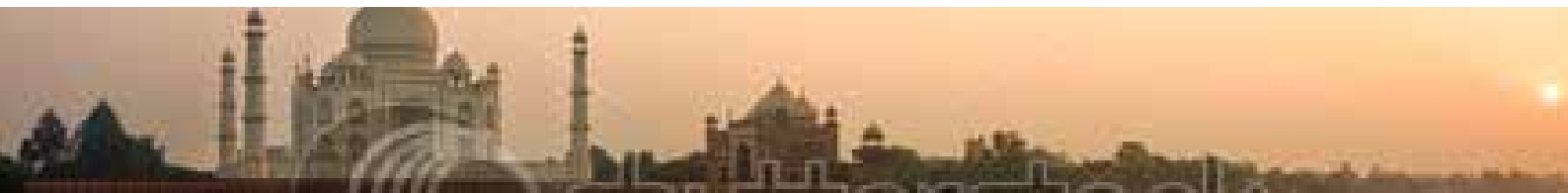
- licensing provisions
- contractual restraints on use; and
- contractual requirements to return physical property on which the database resides.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

TOP TIP FOR THOSE WHO EXPLOIT BIG DATA

Under the PDPO, consent of the data subject is required if his/her Personal Data is used for a new purpose. Those who exploit big data (which may contain Personal Data) should therefore consider data protection issues up front as the Personal Data may not be able to be used in the manner they wish unless the prior consent of the data subject has been obtained. Marketing databases which contain Personal Data can only be sold with the written consent of all the data subjects to which the Personal Data relates, unless the Personal Data of the non-consenting data subjects is excised.



- Australia
- Austria
- Belgium
- Brazil
- China
- EU
- France
- Germany
- Hong Kong
- India**
- Italy
- Japan
- The Netherlands
- Romania
- Singapore
- South Africa
- South Korea
- Spain
- Turkey
- UK
- USA

10. INDIA

KEY CONTACTS



Sajai Singh
Partner
T +91 98 450 78666
sajai@jsalaw.com



Soumya Patnaik
Associate
T +91 80 4350 3623
soumya.patnaik@jsalaw.com



Probir Roy Chowdhury
Partner
T +91 80 4350 3618
probir@jsalaw.com

ORIGINAL DATABASES

Protected? Yes. Databases are protected by copyright, as ‘literary works’. Literary work has been defined as including “computer programs, tables and compilations, including computer databases.”

Ownership The protection is given to the author/creator of the database.

Pre-conditions Copyright law only protects original databases. In order to determine whether a database is ‘original’, the courts in India have constantly relied on the ‘sweat of the brow’ doctrine, thereby protecting compilations/databases solely on the ground that the author had devoted time, money, labour and skill in creating it, even though there was no uniqueness in the arrangement of the data. However, this doctrine has been questioned by the Delhi High Court in the case of *Eastern Book Co. v. Navin J Desai*²², where it refused to apply this doctrine and, instead, applied the ‘modicum of creativity’ rule to satisfy the test of originality. Accordingly, the current position in India is that in order to be protected under copyright, the compilation/database should be ‘original’, satisfying the ‘creativity’ criteria.

May cover (a) Law Reports (reports of judgments) as long as the reporter has created a composite document along with head-notes, editorial comments, footnotes, setting, layout, presentation, etc.; (b) List of clients and addresses arranged and designed by an organisation.

Unlikely to cover Telephone directories (simple listing of numbers).

²² (2002) 25 PTC 641 (Del) (DB)



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Duration Term of copyright in literary works published within the lifetime of the author subsists for the life of the author plus 60 years from the year following the year in which the author dies. However, there has been no clear pronouncement by Indian courts regarding the ‘term’ of copyright specifically in databases.

Scope of Protection Infringement will arise by temporarily or permanently reproducing the database, including storing it in any medium by electronic means, issuing copies of the database to the public, or communicating it to the public, to make any translation or adaptation of the database.

Remedies include injunctions, damages or account of profits. Criminal proceedings may also be initiated, and the Copyright Act 1957 (the “Act”) provides for punishment by imprisonment for a minimum term of 6 months and a maximum term of 3 years, with a fine which may vary from a minimum of Rs. 50,000 to Rs. 200,000.

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

There is no separate protection for databases in which an investment has been made. Copyright law only protects original databases. See section above.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

CONFIDENTIAL DATABASES

There is no specific statute that protects confidential information from misappropriation, other than via contractual obligations under Confidentiality and Non-Disclosure Agreements. Any contractual breach could be remedied through an action for damages and/or an injunction.

PERSONAL DATA

Is personal data given particular protection? Yes, under the Information Technology Act, 2000 (the “**IT Act**”) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (“**Privacy Rules**”).

Who can rely on it? Individuals who are the subject of the personal data (“**Data Subjects**”) are protected by the IT Act and the Privacy Rules. Data Subjects have to grant their prior express consent for collection, processing, storage, transfer, use, or disposal of their Sensitive Personal Data or Information (“**SPDI**”). Further, they have the right to access their SPDI, and correct their information at any time, or withdraw their consent to its use at any time.

What data? The Privacy Rules strictly protect only a category of personal data known as Sensitive Personal Data or Information SPDI which consists of (a) password; (b) financial information such as Bank account or credit card or debit card or other payment instrument details; (c) physical, physiological and mental health condition; (d) sexual orientation; (e) medical records and history; (f) biometric information; and (g) any detail relating to these categories of information.

Scope of protection The Privacy Rules regulate the processing of SPDI, mainly through imposing obligations of procuring express consent of Data Subjects, as well as maintaining reasonable security practices and procedures of the minimum standards of IS/ISO/IEC 27001. This could limit what the owner of a database can legitimately do with the database, especially in terms of using the SPDI information in the database, transferring it to third party service providers, etc.

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

There are no other types of protection for data or databases.

SIGNIFICANT RECENT CASES

There have been no significant recent cases. The current stance as per case law is that there is required to be a modicum of creativity, however minimal, in order to grant copyright protection to databases.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

UPCOMING LEGISLATIVE CHANGES

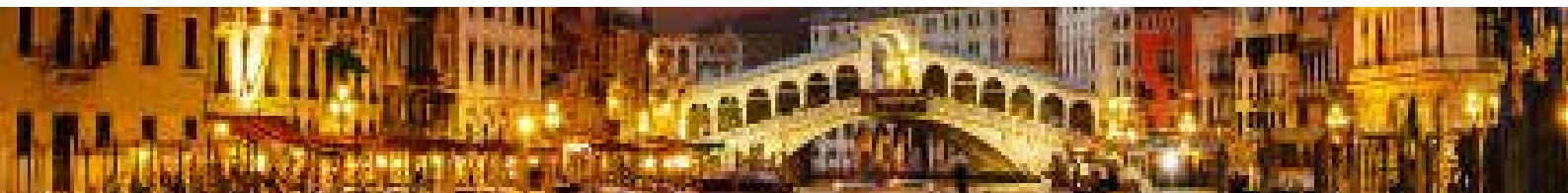
A Right to Privacy Bill is currently being drafted, and is yet to be approved by the Law Ministry of India.

TOP TIP FOR DATABASE OWNERS

Enter into clear and unambiguous confidentiality agreements to protect confidential information and trade secrets.

TOP TIP FOR THOSE WHO EXPLOIT BIG DATA

Consider personal data protection issues (regarding permissible use, transferability, storage rights, etc.) while acquiring a database.



- Australia
- Austria
- Belgium
- Brazil
- China
- EU
- France
- Germany
- Hong Kong
- India
- Italy**
- Japan
- The Netherlands
- Romania
- Singapore
- South Africa
- South Korea
- Spain
- Turkey
- UK
- USA

II. ITALY

KEY CONTACTS



Roberto Valenti
 Partner
 T +39 02 80 618 518
 roberto.valenti@dlapiper.com



Stefania Baldazzi
 Associate
 T +39 02 80 618 616
 stefania.baldazzi@dlapiper.com



Gianluigi Marino
 Associate
 T +39 02 80 618 654
 gianluigi.marino@dlapiper.com

The law is part harmonised with general EU law (see EU section). In this section we therefore only highlight areas that differ from EU-wide law.

ORIGINAL DATABASES

Protected? Italy is subject to the EU wide Database Directive 96/9 (see EU section), implemented in Italy by Italian Copyright Law (ICL), Law. No. 633/1941 (the link is to an unofficial English translation). The definition of “database” is set out in Section 2, N. 9, Section 64 quinquies and Section 64 sexies of the ICL.

May cover Based on case law, databases that result from an original selection of data and material, with a complex structure.

Unlikely to cover A list of clients arranged by name and addresses, databases including all data and material available on a certain topic (e.g. a telephone directory) and databases with alphabetical or chronological order or other non-original elements as selective criteria.

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Protected? In Italy, there is protection with the *sui generis* right under Section 102 bis of the ICL (see EU section above).

May cover Telephone directories in the event that a relevant investment has occurred (in the collection of all the consent from the subjects); a football fixture list (upon the same condition).

Unlikely to cover A collection of funny and ironic SMS messages.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

CONFIDENTIAL DATABASES

Protected? According to Section 98 of the Italian Industrial Property Code (Legislative Decree No. 30/2005, “**IIPC**”) regulating trade secrets, company information and technical/industrial knowhow, including commercial information, under the legitimate control of the holder, are protected, provided the pre conditions listed below are met.

Alternatively, Section 2598 of the Italian Civil Code prevents use of unfair competition practices that are non compliant with professional fairness and cause harm to another company. Use of a confidential database may result in an unfair commercial practice.

Ownership Rights belong to the holder of the confidential database.

Pre-conditions Information is protected under the IIPC where it:

- is secret (not generally known or accessible to the public);
- has an economic value given the secrecy; and
- is subject to measures taken by its holder which are reasonably adequate to keep them secret.

May cover Commercially sensitive databases.

May not cover Collection of information which are publicly accessible.

Duration From creation of the information until disclosure to the public.

Scope of protection The holder of the IIPC rights can exclude parties from acquiring, revealing or using the information or knowhow unless consent is given or third parties have independently acquired the information/knowhow. The holder of a database can prevent competitors from using the database unless the third party has independently acquired the data or the data has been published or licensed without imposing confidentiality.

Remedies Injunctions, recall or destruction of infringing materials or materials used to create infringing copies, damages and reimbursement of legal costs.

PERSONAL DATA

Is personal data given particular protection? The handling of personal data is subject to the [Italian Data Protection Law No 196/2003](#) (link is to English translation).

(Also, see [EU section](#) above.)

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

No.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

SIGNIFICANT RECENT CASES

Trib. Bologna Sez. spec. propr. industr. ed intell., 10/08/2011 (*Porfiri G. c. Franca Cosimo Panini Editore S.p.A.*). A collection of funny and ironic SMS messages was held not to be a database under the ICL, and so did not qualify for the database rights.

Corte appello Milano Sez. spec. propr. industr. ed intell. 21/11/2011, No. 3206 (*R.C.B.F v. A. B. and S.A.G.I.*). This decision considered whether the *sui generis* database rights (under Section 102 *bis* ICL) protects a database consisting of a book containing genealogical information. It was held that such a book could be protected by database rights, provided that there had been substantial investment in obtaining the contents of the book.

Trib. Roma, Sez. spec. propr. industr. ed intell. 01/10/2008 (*Pre View S.a.S. C. Wyeth Lederle S.p.A. and others*). DLA Piper Italy represented Pre-View S.a.S. in this case obtaining a finding of infringement of database rights and unfair competition in respect of the use of a pharmaceutical database by a competitor. The assignee of the competitor, however, was considered not liable since the use of the database was made according to a contract lawfully entered into by the assignee with the third party competitor, which had warranted that it was the rightful owner of copyright in the database; this released the assignee from any liability.

UPCOMING LEGISLATIVE CHANGES

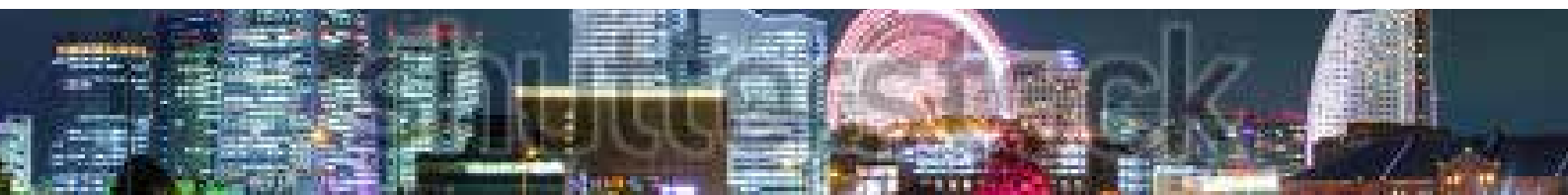
See [EU law section](#).

TOP TIP FOR DATABASE OWNERS

Regulate confidentiality in agreements providing access to confidential databases, also including penalties in case of infringement. Ensure written NDAs are in place with all those given access to confidential databases. When databases include personal data, ensure that data have been collected and transferred in compliance with data protection laws. It could be possible to own a database which cannot be lawfully exploited, especially with reference to sensitive data and, in general, for marketing purposes.

TOP TIP FOR THOSE WHO EXPLOIT BIG DATA

Consider personal data protection issues when exploiting a database, with reference both to data protection law and local Data Protection Authority decisions.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

12. JAPAN

KEY CONTACTS



Henry Koda
Partner
T +81 3 4550 2824
henry.koda@dlapiper.com

ORIGINAL DATABASES

Protected? Databases may be protected by copyright if, by reason of the selection or systematic construction of information contained therein, they constitute intellectual creations, under the **Japanese Copyright Act 1970** (“Act”). Advanced creativity is not required in Japan for protection as a copyright work, and most databases are considered to be protected under the Act.

Ownership The database author(s)/creator(s) (Article 2, paragraph 1, item 2 of the Act) are the owners of the rights and protection.

Pre-conditions The database must:

- (i) satisfy the definition of “Database” prescribed in Article 2, paragraph 1, item 10-3 of the Act, under which “Database” means a collection of information, such as dissertations, numerical values or diagrams, which is systematically organized so that such information can be searched by use of a computer; and
- (ii) constitute intellectual creations, by reason of the selection or systematic construction of information contained therein (Article 1.2-2, paragraph 1 of the Act).

There is no requirement for a copyright notice or registration (Article 17, paragraph 2 of the Act).

May cover telephone directory sorted by occupation or marketing databases with a complex structure.

Unlikely to cover case law search databases covering all precedents posted on the published digest.

Duration Copyright protection starts at the time of database creation (Article 51, paragraph 1. of the Act). Protection generally lasts for the life of the author plus 50 years (Article 51, paragraph 2 of the Act) after the end of the calendar year in which such author dies (Article 57 of the Act).

Scope of Protection Infringement results from doing the following:

- temporary or permanent reproduction;
- a translation, adaptation or other alteration;
- distribution or communication to the public of the database or copies of it; or
- reproduction, distribution, communication, display to the public of the results of the above acts.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Remedies include Injunctions (Article 112 of the Act), presumption of amount of damages (Article 114 of the Act), measures for restoration of honour (Article 11.5 of the Act) and penal provisions listed under Articles 119 – 124 of the Act.

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Databases in which investments have been made do not receive separate protection beyond the protection described above or under contractual obligations.

CONFIDENTIAL DATABASES

It is possible for confidential databases to be protected by certain specific laws (e.g. Unfair Competition Prevention Act, Civil. Code, Penal Code etc.). There is no specific law which protects confidential databases in Japan.

PERSONAL DATA

Is personal data given particular protection? The handling of “Personal Information” is subject to the [Act on the Protection of Personal Information](#) (“APPI”).

Who can rely on it? The individual who is the subject of the personal information.

What data? “Personal Information” is defined in Article 2, paragraph 1 of the APPI as information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including information that will allow easy reference to other information and thereby enable the identification of the specific individual).

The APPI also defines “Personal Information Database, etc.” in Article 2, paragraph 2, as an assembly of information systematically arranged in such a way that specific Personal Information can be retrieved by a computer; or an assembly of information designated by a Cabinet Order as being systematically arranged in such a way that specific Personal Information can be easily retrieved. The term “Personal Data” is defined in Article 2, paragraph 4 of the APPI as Personal Information constituting a Personal Information Database, etc.

Scope of protection The legislation regulates the usage of Personal Data by business operators handling Personal Information. The following are the main provisions for the protection:

- Specification of the purpose of use (Article 15);
- Restriction by the purpose of use (Article 16) a Proper acquisition (Article 17);
- Maintenance of the accuracy of data (Article 19);
- Supervision of employees (Article 19); and
- Restriction of provision to a third party (Article 23).

If business operators handling Personal Information do not follow the regulations, such acts are subject to criminal charges.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA

On 28 March 2002 the Tokyo District Court ruled that even if a database is not protected under the Japanese Copyright Act, the reproduction of such database may constitute a tort in certain circumstances under Article 709 of the Civil Code. Tokyo Dist. Ct. Mar. 28, 2002, Hei 8 (wa) no. 10047, 1793 HANREI JIHO 133 (Japan).

Also, the **Act on the Protection of Personal Information Held by Administrative Organs (APPIHAO)** was made in order to protect the rights and interests of individuals while achieving proper and smooth administrative management, in view of a significant increase in the use of Personal Information by administrative bodies, by providing for basic matters concerning the handling of personal information by such bodies.

Under the APPIHAO, the same definition for “Personal Information” is used (Article 2, paragraph 3 of the APPIHAO) and there are specific requirements relating to retention of Personal Information (Article 3 of the APPIHAO), clear indication of the purpose of use (Article 4 of the APPIHAO), and maintenance of accuracy (Article 5 of the APPIHAO) when administrative bodies handle Personal Information.

SIGNIFICANT RECENT CASES

There have not been any significant recent cases in respect of rights in data/databases in Japan.

UPCOMING LEGISLATIVE CHANGES

Currently, we do not foresee any amendment or legislation regarding database protection.

In order to promote fair use of copyright works and secure protection of copyright, the Japanese Copyright Act was amended in June 2012.

With respect to databases, the Institute of Intellectual Property has carried out research on protection of intellectual property rights of database creators²³. In 2001, the Science Council of Japan opposed the enactment of legislation on the sui generis right²⁴. Its reason was that it would interfere with the academic, cultural and economic development of the country.

TOP TIP FOR DATABASE OWNERS

In Japan, there is no specific statute which governs database protection like the EU Database Directive. However, databases that constitute intellectual creations by selection or systematic construction can benefit from copyright protection. Moreover, databases which are not protected under the Copyright Act due to lack of creativity can potentially be protected by general tort rules.

²³ The research result (in Japanese) can be obtained from www.iip.or.jp/summary/pdf/detail06j/18_15.pdf

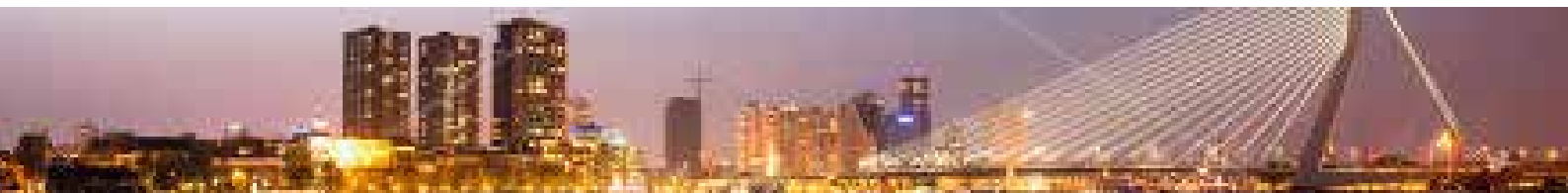
²⁴ The statement (in Japanese) can be obtained from www.scj.go.jp/info/kohyo/pdf/kohyo-18-k136.pdf



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

TOP TIP FOR THOSE WHO EXPLOIT BIG DATA

Database owners should be careful about the status of Japanese law and regulations because the Japanese Government is now discussing amending the APPI so that entities can use big data more effectively. For instance, under the current APPI, a database owner cannot provide a third party with personal information without getting permission from the individual but the Act may be amended in 2015 so that the database owner can provide the personal information without permission if the information is made anonymous.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

13. THE NETHERLANDS

KEY CONTACTS



Alexander Tsoutsanis
Advocaat
T +31 20 541 9994
alexander.tsoutsanis@
dlapiper.com



Robin de Wit
Advocaat
T +31 20 541 9674
robin.dewit@dlapiper.com

The law is part-harmonised with general EU law (see [EU section](#)). In this section we therefore only highlight areas that differ from EU-wide law.

ORIGINAL DATABASES

Protected? Under Dutch law, original databases are protected under art. 10(3) of the Copyright Act. This is in conformity with the EU-wide Database Directive (see [EU section](#)). Even prior to the enactment of the Directive, the Dutch Supreme Court afforded similar copyright protection to databases, applying a test which is similar to the EU threshold requirement that the collection of the database constitutes an “intellectual creation of the author”²⁵.

Remedies Right holders of such original databases are entitled to the usual remedies against copyright infringement, warranting both injunctive and monetary relief. Injunctive relief is also available in the shape of ultra-fast temporary restraining orders (usually granted within 24 hours), which can be particularly helpful in internet cases.

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Protected? In The Netherlands, protection is provided in the so-called Databases Act (*Databankenwet*), which implements the EU-wide Database Directive (see [EU section](#)). The Netherlands has seen increased industry activity and also increased litigation in the field of database protection. Much attention centred on the so-called (in)admissibility of dedicated search engines re-utilizing data from information portals involving real estate (eg *Zoekallehuizen.nl*; *Jaap.nl*; *EI Cheapo*) and used cars (*Gaspedaal*)²⁶.

²⁵ Dutch Supreme Court 4 Jan. 1991, NJ 1991, 608 (Van Dale/Rome).

²⁶ Dutch Supreme Court 22 March 2002, NJ 2003, 149 (NVM/Telegraaf); Court of Appeal Arnhem 4 July 2006 LJA0089 (*Zoekallehuizen.nl*), Court of Appeal Amsterdam 13 Dec. 2007 LJA BC0125 (*Jaap.nl*); Court of Appeal the Hague 27 March 2012 IEPT20120327 (*Gaspedaal.nl*).



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Remedies See above. Provided infringement is properly framed the Dutch courts even allow cross-border temporary restraining orders in which the Dutch court grants an ex-parte injunction which extends to the entire EU without the (alleged) infringer being heard. This is particularly helpful in cases of infringing Apps sold on e.g. *iTunes* or *Android*, for example. In such cases, right holders always need to follow-up with *inter partes* proceedings on the merits (unless settlement materializes) and are also sometimes expected to post a bond.

CONFIDENTIAL DATABASES

Protected? The Netherlands provides for protection of confidential databases, primarily on the basis of the general doctrine of tort (art. 6:162 Dutch Civil Code) and the over-arching obligation in art. 39 TRIPs to protect confidential information and trade secrets. A recent example is found in *GBT v Ajinomoto*²⁷. The confidential information itself, is not protected: it is rather the unlawful violation of the obligations of confidentiality which constitutes the tort. This is often accepted in case of breach of contract, abuse of trust and inducements to violate confidentiality obligations.

Ownership The protection of confidence may cover the owner of the database, but only in circumstances where the recipient of the information contained owes the owner an obligation to keep the information confidential (i.e. if a reasonable person in the position of the recipient would understand that the information was given in confidence).

Pre-conditions The information needs to be “confidential”, in the sense that the information was not generally known, and the owner of the confidential database took reasonable measures to safeguard such confidentiality.

Duration Protection arises from the time the obligation of confidence arises (providing the confidential database) and lasts until the obligation ceases (usually until the information passes into the public domain).

Remedies Injunctions (interim and final), damages and/or destruction.

PERSONAL DATA

See [EU law section](#). The Netherlands implemented the EU Data Protection Directive 95/46/EC on 1 September 2001 with the Dutch Personal Data Protection Act (“**Wbp**”). Enforcement is through the Dutch Data Protection Authority (“**College Bescherming Persoonsgegevens**”).

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

No.

²⁷ Court of Appeal The Hague 29 March 2011 IEF 9507 (*GBT/Ajinomoto*).



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

SIGNIFICANT RECENT CASES

Autotrack v Gaspedaal.nl involved a case where a dedicated search engine provided by *Gaspedaal* re-utilized data from the *Autotrack* database. The Court of Appeal referred no less than 9 questions for clarification by the [European Court of Justice](#) (case C-202/12), focusing on when the extraction and/or re-utilization involves a substantial or insubstantial part of the contents of the database involved, as mentioned in art. 7(1) and (5) of the EU Directive. The CJEU rendered a decision on 19 December 2013. In short, it was held that the whole or a substantial part of the content is re-utilized where the dedicated meta search engine comes close – by resembling the database – to the manufacture of a parasitical competing product (recital 42 of the Database Directive), but without actually containing the data. This decision effectively bans the “scraping” of databases.

PR Aviation v Ryanair the Supreme Court confirmed the position of the Court of Appeal regarding the decision that Ryanair’s database containing data on its flights did not qualify as a database ‘in which a substantial investment had been made’. Furthermore, the Supreme Court denied Ryanair’s statement that its collection of data qualified as an ‘original database’, since it could not meet the requirement of originality. The protection of writings (*geschriftenbescherming*) as a mitigated form of copyright protection was rejected (art. 10 sub 1 (1) Dutch Copyright Act). According to art. 24a sub 3 Dutch Copyright Act, the statutory restriction regarding lawful use necessary for the purposes of access to the contents of the database (art. 6 Directive) cannot be excluded by contract. Ryanair’s Terms of Use contained such exclusion. Since Ryanair’s data collection was neither protected by copyright law, nor by database law, the Supreme Court referred one question for clarification by the European Court of Justice, focusing on the examination of whether the prohibition on contractual exclusion of that restriction also applies to non-protected databases. We are still awaiting the CJEU’s judgment.

UPCOMING LEGISLATIVE CHANGES

See [EU section](#).

TOP TIP FOR DATABASE OWNERS

Documentation is key: documenting the investments and structure underlying your database is as important as building the database itself. How the information is arranged and made accessible and how much you have invested is critical to invoke protection. Lack of such evidence is often a cause for delay or difficulty in enforcing your rights in the database later on.

TOP TIP FOR THOSE WHO EXPLOIT BIG DATA

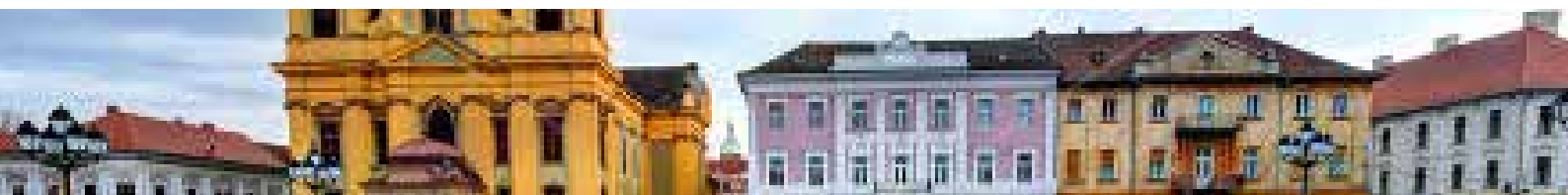
Concerns related to Big Data lie primarily within the scope of data protection (there are conditions attached to the processing of personal data), but also of unfair commercial practices. To make the most out of your Big Data, gain customer confidence and, to enable the widest use of the data, the following points need to be considered:

1. Notification of the Dutch Data Protection authority (depending on the use of Big Data);



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

2. Transparency, and thus, complete, accurate and adequate information, is of paramount importance. Notification of data subjects on the collection of personal data, consenting to individual profiling and encouraging and inviting a process for customers to access, review and correct information that has been collected about them in order to secure the best safety net for accuracy of personal data;
3. Since data is generated and collected through an amazing array of sources, security is of the essence. It is not enough to implement standard general security contractual clauses. Filtering, cleansing, pruning, conforming, matching, taking care of appropriate storage, joining, logging, monitoring, diagnosing should be applied at the earliest touch points possible. Also, data security professionals need to take an active role early in the decision making process in order to avoid data security risks and fines; and
4. Dealing with cross-border data transfers and ensuring the compliance of international data transfers. This could entail developing and filing Binding Corporate Rules, entry into the EU-US Safe Harbor, or incorporating EU Model Clauses into the organization's operations all around the world.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

14. ROMANIA

KEY CONTACTS



Cosmina Simion
Head of IP, Media and
Technology
T +40 372 155 816
cosmina.simion@dlapiper.com



Laura Leanca
Associate
T +40 372 155 814
laura.leanca@dlapiper.com

ORIGINAL DATABASES

Protected? The **EU-wide Database Directive 96/9** is implemented in Romania through the Romanian **Copyright Act no. 8/1996**, (“**Copyright Act**”). An unofficial translation of the Copyright Act (updated as of 1 December 2012) is available on the website of the Romanian Copyright Office (see <http://www.orda.ro/default.aspx?pagina=650>).

Pre-conditions Original databases (separately from their content) must fulfil the originality threshold (“author’s own intellectual creation”, see **EU section**).

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Protected? Similarly to the EU Database Directive 96/9, Articles 122¹ – 122⁴ of the Copyright Act stipulate a sui-generis right for the maker of the database (the person who takes the initiative and the risk of investing), provided that the criteria set out in the **EU section** are met.

CONFIDENTIAL DATABASES

Protected? In Romania, there is no general legal framework protecting the misuse of confidential information. Therefore, database owners should ensure that appropriate NDAs have been put into place.

However, the Romanian Civil Code (Article 1184) grants protection to confidential information, when this is communicated by a party during any contract negotiations. The other party is not allowed to disclose such information to third parties and/or use it for its own interest, irrespective of whether any agreement is concluded. Furthermore, the parties to an agreement are bound to act in good faith both during the contract negotiations and for the duration of the agreement. Such non-disclosure obligation cannot be subject to limitation or exclusion.

Moreover, according to the Romanian Unfair Competition Act no 11/1991 (“**Unfair Competition Act**”), as recently amended by the new Romanian Criminal Code, the following actions constitute a criminal offence: (i) the disclosure or use of trade secrets by third parties, following an industrial or commercial espionage; (ii) the disclosure of trade secrets by persons



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

empowered by the holders of confidential information for the purposes of representing them in front of public authorities; (iii) the use of trade secrets by public servants. A prerequisite for any sanction is, apart from the specific conditions required under criminal law, evidence proving that the interests of a natural person or legal entity have been affected. The sanction is either imprisonment from 3 months to 2 years or a criminal fine.

Ownership Rights belong to the holder of the confidential information and trade secrets.

Pre-conditions Trade secrets are protected where they are: (i) a defined information/method; (ii) confidential (i.e. they are not of common knowledge or are not easily accessible to the persons pertaining to the environment usually dealing with this sort of information); (iii) have an economic value due to their secrecy; and (iv) the owner of the information has taken reasonably adequate measures to preserve them as secret.

May cover Client databases.

May not cover Publicly available databases.

Duration From creation until the information is made public.

Scope of Protection Owners of confidential information may prevent third parties from disclosing or using it for any purpose without the owner's consent. However, confidentiality obligations do not apply where third parties have independently acquired the respective information.

Remedies Injunction, destruction of infringing materials, damages, legal costs.

In case the database (and its content) is protected under a confidentiality agreement, the common legal remedies under contract law apply (article 1549 of the Romanian Civil Code). The aggrieved party has the choice either (i) to enforce the further execution of the contract by its contract party and to claim compensation for damages suffered, if any, or (ii) to request the termination of the agreement for breach of the other party's contractual obligations in conjunction with a claim for damages.

PERSONAL DATA

See [EU section](#). The general legal framework is set out in Act no. 677/2001 on the protection of individuals with regard to the processing of their personal data and the free movement of such data, implementing the [EU Data Protection Directive 95/46](#). An unofficial translation of Act no. 677/2001 is available on the website of the Romanian Data Protection Authority ([here](#))

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

Generally no.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

SIGNIFICANT RECENT CASES

While Romanian courts have not yet been faced with a large amount of litigation, they follow the principles set out by the **CJEU** in its already established case law.

In 2007, the Bucharest Tribunal ruled that the display by the defendant on its website of a photograph extracted from the claimant's website (which comprised 2000 images) did not amount to a substantial extraction, from both a qualitative and a quantitative perspective. The Bucharest Court of Appeal upheld the Tribunal's decision. The court cited the ECJ's ruling in *British Horseracing Association v William Hill*.

UPCOMING LEGISLATIVE CHANGES

The new Romanian Criminal Code and Criminal Procedure Code entered into force on 1 February 2014. The penalty for improper use of confidential information under the Unfair Competition Act was modified: imprisonment is now possible from 3 months to 2 years (previously "6 months to 2 years").

Moreover, the Romanian Competition Council intends to imminently amend the Unfair Competition Law*. However, no substantial changes are envisaged in relation to the protection of trade secrets.

In case the European Commission's proposal for a directive on the protection of trade secrets will pass into law, Romania will have to implement it into national legislation.

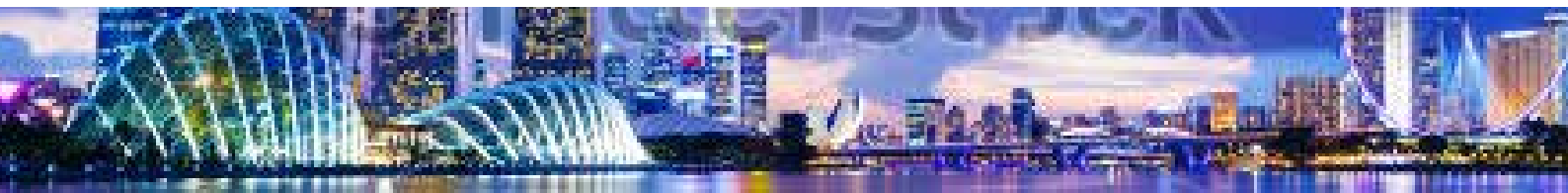
TOP TIP FOR DATABASE OWNERS

Do not disclose confidential information to third parties, unless they have executed an NDA that provides for the payment of penalties for non-authorized disclosure.

TOP TIP FOR THOSE LOOKING TO EXPLOIT BIG DATA

In order to benefit from the copyright and sui-generis protection of databases, ensure that the database comprising the data you want to exploit meets the criteria for protection and make sure you have acquired all rights in respect of the data to be compiled therein.

* This chapter is up-to-date as of 9 August 2014. It may be that this new legislation enters into force by the end of August 2014.



- Australia
- Austria
- Belgium
- Brazil
- China
- EU
- France
- Germany
- Hong Kong
- India
- Italy
- Japan
- The Netherlands
- Romania
- Singapore**
- South Africa
- South Korea
- Spain
- Turkey
- UK
- USA

15. SINGAPORE

KEY CONTACTS



Scott Thiel
 Partner
 T +85 221 030 519
 scott.thiel@dlapiper.com



Yvonne Lee
 Counsel – TSMP Law
 Corporation
 T +65 6216 9950
 yvonne.lee@tsmp.com.sg

ORIGINAL DATABASES

Protected? Original databases created by an identified human author may be protected in Singapore by copyright as a ‘literary work’ which includes a computer program and a compilation in any form (e.g. ‘a compilation, or table, of data other than relevant materials or parts of relevant materials which, by reason of the selection or arrangement of its contents, constitutes an intellectual creation’) under the [Singapore Copyright Act](#) (Cap 63, 2006 Rev Ed) (“Act”).

Ownership The database author(s) is/are the first owner(s) of the copyright, unless made by an employee or employees within the scope of the author’s employment (in which case the employer is considered the first owner).

Pre-conditions As a literary work a database must be “original” – meaning that there is a degree of independent effort in the creation of the work. The test for compilation is the same, namely that of originality whether there is sufficient amount of skill, labour and judgment involved in the creative process. There is no need to file for registration to obtain copyright protection in Singapore.

May cover Marketing databases with complex structures based on careful analysis of specific customer or business needs, assuming that the individual authors can be identified.

Unlikely to cover Essentially, any collection of information/data which has no element of “originality”. For example, databases which consist of readily available information or which are licensed on terms which do not impose obligations of confidentiality. For any copyright to subsist in a compilation, the selection or arrangement of its contents must be the product of intellectual creation.

Duration Generally, copyright protection in a literary work such as a database will automatically arise as soon as it is expressed or fixed in a material form (e.g. paper, electronic, tape and film) from which it is capable of being reproduced. The protection subsists during the life of the author plus 70 years after the calendar year of the author’s death.

Scope of Protection Infringement will arise through reproducing the work in a material form, publishing the work, meaning making it available to the public, or making any copy and/or adaptation of the work without the consent of the copyright owner. Such actions are “primary



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

infringements”. The owner’s rights are also infringed by “secondary infringements” such as importing, selling, offering for sale and exhibiting in public any works where the infringer knows, or reasonably ought to know, that the works have been made without the copyright owner’s consent; falsely attributing the authorship of a work or the identity of the creator of the database; and falsely removing or altering the rights management information electronically attached to a work.

However, in relation to databases specifically, as legislation protects only the original expression of ideas and not the facts or data per se, it may be possible for someone to extract data from a work and yet not infringe copyright as long as the work is not reproduced in the same arrangement or presented in the same form.

Remedies: Remedies include injunctions, damages or an account of profits, an order for delivery up and/or disposal of infringing works in relation to the copyright. Criminal proceedings may be initiated for primary and/or secondary infringements. If a primary infringement is wilful and significant and undertaken in order to obtain a commercial advantage, remedies can include a fine not exceeding S\$20,000 and/or imprisonment not exceeding 6 months. Repeated offences attract penalties of fines up to S\$50,000 and/or 3 years imprisonment. Secondary infringements can attract penalties ranging from a fine of S\$10,000 per incident (S\$100,000 in aggregate) and/or imprisonment not exceeding 5 years.

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Databases in which investments have been made do not receive protection beyond those described herein. The most effective way to protect databases which do not qualify for copyright protection is via contractual terms that cover restrictions around access and use of the data and database as a whole.

CONFIDENTIAL DATABASES

The laws of Singapore allow for the protection of works, including databases, classified as “confidential information”, being information that has not been made available to the public. Section 6 of the Act states: *Nothing in this Act shall affect the operation of the law relating to breaches of trust or confidence.*

Information will be protected as confidential if and so far as: (i) the information to be protected has the necessary quality of confidentiality or (ii) the information had been imparted in circumstances importing an obligation of confidence. Such confidential information is protected against any unauthorised use of the information to the detriment of the party who originally communicated it.

Again, the scope of protection is offered only in this limited context. A work, such as a compilation, does not get protected on its merits, but rather as a result of the continued confidentiality of the information shared between parties with an obligation to secrecy.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

PERSONAL DATA

Is personal data given particular protection? Yes, under the [Singapore Personal Data Protection Act 2012](#) (“**PDPA**”).

Who can rely on it? Individuals who are the subject of “Personal Data”.

What data? Personal Data is defined as data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which an organisation has or is likely to have access. Business contact information which is not provided by the individual solely for his personal purposes, is excluded.

Scope of protection The PDPA regulates the collection, retention, correction, access, use and disclosure (including overseas transfer) of Personal Data by organisations which include individuals not acting in personal or domestic capacity and corporates but exclude public agencies such as the Singapore Government, statutory bodies and authorities. The PDPA also regulates the sending of specified messages (e.g. marketing messages, excluding business to business messages, research and surveys) to Singapore telephone numbers (calls, telefaxes and SMS/MMS).

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

There are no other types of legal protection for data or databases. Separate legal regimes govern data amounting to official secrets.

SIGNIFICANT RECENT CASES

The Singapore Court of Appeal in the recent case, *Asia Pacific Publishing Pte Ltd v Pioneers & Leaders (Publishers) Pte Ltd* [2011] 4 SLR 381, stated that, inter alia, in order for any copyright to subsist in a compilation, the selection or arrangement of its contents had to be the product of intellectual creation, and an author had to be first identified before the work in question could be deemed original.

UPCOMING LEGISLATIVE CHANGES

No expected changes relating to databases are expected at the time of writing.

TOP TIP FOR DATABASE OWNERS

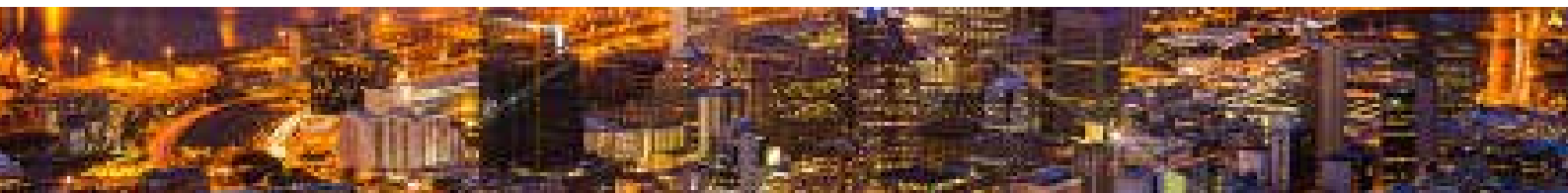
1. Ensure that contracts with third parties who undertake tasks in relation to a database on your behalf (e.g. collecting, gathering, organising information/data) are clear on the ownership rights to the database. In addition, publicly available databases must have appropriate terms of use to ensure users have appropriate contractual obligations in relation to the information they access/use.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

TOP TIP FOR THOSE WHO EXPLOIT BIG DATA

1. Legal issues in Singapore will depend on the purposes for which big data is to be exploited. Potential issues include violation of web access terms, infringement of copyright, and privacy law issues including personal data violation. Database owners should document their data sources and life cycle, as it is likely that there are a few so-called authors, collectors and disclosers.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

16. SOUTH AFRICA

KEY CONTACTS



Preeta Bhagattjee

Director
T +27 11562 1038
preeta.bhagattjee@
dlacdh.com



Simone Gill

Director
T +27 11562 1249
simone.gill@dlacdh.com

ORIGINAL DATABASES

Protected? Original databases are protected by copyright in South Africa in that they constitute ‘literary works’ defined under section 1 of the South African *Copyright Act 98 of 1978* (“**Copyright Act**”) to include, ‘tables and compilations, including tables and compilations of data stored or embodied in a computer or a medium used in conjunction with a computer.’

Ownership In terms of the Copyright Act, first ownership in the copyright of a database shall vest in the author or, in the case of a work of joint authorship, in the co-authors of the database, provided that if the database was created by an employee in terms of a contract of employment, the employer will be the owner of the copyright in the database.

Pre-conditions Under the Copyright Act, copyright arises upon creation of the work qualifying for copyright and no registration is required. A database qualifies for copyright protection in terms of the Copyright Act if –

- (i) it is ‘original’. The term ‘original’ has not been defined in the Copyright Act but its interpretation has been developed through the common law. In order for a database to meet the originality threshold, the creation of the database must have been a product of ‘substantial skill, judgement and labour’ and must not be trivial or a purely mechanical exercise. A database may be entitled to copyright protection under the Copyright Act even if its creation or any other act in relation thereto involved an infringement of copyright of an original database provided that, when considered in its entirety, it is substantially different from the original database;
- (ii) it is reduced to physical or material form;
- (iii) the author is (a) a South African citizen or is domiciled or resident in the Republic (in the case of an individual); (b) a body incorporated under the laws of the Republic of South Africa (in the case of a juristic person); or it is first published in South Africa, (i.e. where the author does not fall within either of the categories described in (a) and (b) above).



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

May cover Compilations of data relating to a set of codes or numbers used for identification purposes; and data structures which represent improvement or refinement of already published data structures protected by copyright.

Unlikely to cover Computer-generated databases in which there was no human authorship involved in creating the database; and database compilations that simply copy or make trivial changes to the first or more databases.

Duration The period of copyright protection continues for the lifetime of the database author plus 50 years from the end of the calendar year in which the author dies, unless the database has not been published prior to the death of the author, in which case copyright will subsist for a period of 50 years from the end of the year in which the database is first published.

Scope of Protection In terms of the Copyright Act, copyright in a database confers an exclusive right on the owner (being the author of the database) to reproduce, adapt or publish the database (or authorise such reproduction, adaptation or publication). Copyright shall be infringed by any person, not being the owner of the copyright, who, without licence of such owner, does or causes any other person to perform any act in South Africa which the owner has the exclusive right to do or authorise, although a number of exceptions are provided for under the Copyright Act, including any reproduction, adaptation or publication for purposes of fair dealing, including for (i) research, private study, personal or private use; (ii) review or criticism or for the purpose of reporting current events (provided that the name of the author and the source shall be mentioned); (iii) judicial proceedings; and/or (iv) quotation.

Remedies include Damages, interdict, orders for the delivery of infringing copies. In lieu of damages, the owner of the copyright may elect to be awarded a reasonable royalty which would have been payable by a licensee in respect of the work or type of work concerned.

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Databases in which investments have been made do not receive protection other than as described above and below or protections which may be agreed to in terms of a contractual obligation (if any).

CONFIDENTIAL DATABASES

Protected? Databases may be afforded copyright protection in accordance with the provisions above. Confidentiality is a separate issue which may be governed and protected in terms of the common law, rights of privacy and/or a contractual arrangement; or which may arise by virtue of a relationship or duty (including, for example, a fiduciary position and the relationships between employer and employee, doctor and patient, attorney and client and bank and customer). As we have addressed copyright above, we will focus on confidentiality for purposes of this section.

Ownership In addition to the comments above, any database which by its nature is or ought reasonably to be identifiable as confidential and proprietary to the database owner or which is provided or disclosed by the proprietor in confidence.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Pre-conditions In terms of the common law generally; (i) the information must not be in the public domain/generally known; (ii) the owner of the information must take reasonable measures to maintain the confidentiality of the information; and (iii) the party receiving the information is under a duty to protect the confidentiality of the information. This can also be protected contractually.

May cover Any information which is confidential (i.e. which meets the pre-conditions above) without restriction.

May not cover Databases which are (or lawfully become available) in the public domain or which become available from a source other than the owner of the confidential information which source is lawfully entitled without any restriction on disclosure to disclose such information; or databases which are disclosed pursuant to a requirement or request by operation of law, regulation or court order.

Duration As long as the database remains confidential.

Scope of Protection The scope of protection would need to be considered on a case by case basis as this would be dependent on the nature of the relationship (whether contractual or otherwise) which would determine the extent of the duty of confidentiality.

Remedies To the extent that the database qualifies for copyright protection in accordance with the requirements detailed above, the copyright infringement remedies detailed above will apply. In addition, on the basis of a breach of confidentiality, damages or interdictory relief may be sought as a remedy for a breach of contract or breach of duty of confidentiality.

PERSONAL DATA

Is personal data given particular protection? The South African Protection of Personal Information Act 4 of 2013 (“**POPI Act**”) was assented to in November 2013. Although the effective date of the POPI Act is yet to be proclaimed, its implementation appears to be imminent.

Who can rely on it? Data subjects, defined in POPI Act as persons to whom personal information relates. Data subjects may be either natural or juristic persons.

What data? Personal information including but not limited to:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- Information relating to the education or medical, financial, criminal or employment history of the person;
- Any name, identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- Biometric information of the person;
- Personal opinions, views or preferences of the person.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Scope of protection The POPI Act regulates the processing, collection, access, security, quality, retention, cross-border transfer and further processing of personal information and imposes minimum conditions for the lawful processing of personal information, including in relation to accountability, processing and further processing limitation, purpose specification, information quality, openness, security safeguards and data subject participation. Certain exclusions do apply, including where processing: (i) is required for the conclusion or performance of a contract to which the data subject is party; (ii) complies with an obligation imposed by law on the responsible party; (iii) protects a legitimate interest of the data subject; (iv) is necessary for the proper performance of a public law duty by a public body; or (v) is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied. The Information Regulator established in terms of the POPI Act may also grant exemptions. The POPI Act recognises, *inter alia*, data subjects' right to notification of breach of security, informed consent and the right to withdraw consent/object to processing or further processing. It also addresses data subjects' rights relating to direct marketing.

In addition to personal information generally, provision is made for categories of special personal information (being personal information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject) which may not be processed unless the exceptions under the POPI Act are complied with, including where the processing is: (i) carried out with the consent of the data subject; (ii) necessary for the establishment, exercise or defence of a right or obligation in law; (iii) necessary to comply with an obligation of international public law; (iv) for historical, statistical or research purposes; (v) related to information which has deliberately been made public by the data subject; or (vi) compliant with the specific clauses relating to the identified categories of special information. There is a specific prohibition on the processing of personal information of children unless the exceptions under the POPI Act are met.

The Information Regulator is tasked with monitoring and enforcing compliance with the POPI Act and upon receipt of a complaint may, *inter alia*, launch investigation proceedings. An infringement of the provisions of the POPI Act may have criminal or civil consequences as provision is made in the POPI Act for certain criminal offences (in terms of which any person may be liable to a term of imprisonment or an administrative fine on conviction depending on the nature of the contravention) and also for civil actions.

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

The South African Electronic Communications and Transactions Act 25 of 2002 (“ECT Act”) provides for ‘critical databases’ defined in the ECT act as ‘a collection of critical data in electronic form from where it may be accessed, reproduced or extracted’. ‘Critical data’ for the purposes of the ECT Act is data which the state determines to be of importance to the protection of the national security of South Africa or the economic and social well-being of its citizens. The identification and registration procedure for critical databases is as determined by the Minister of Communications.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Database owners should also be aware of the existence of other legislation including but not limited to: the Financial Intelligence Centre Act, the National Credit Act, the Consumer Protection Act, the Financial Advisory and Intermediary Services Act which include data retention provisions which may be applicable to databases.

SIGNIFICANT RECENT CASES

Anton Charl Haupt t/a Softcopy v Brewers Marketing Intelligence (Pty) Limited and Others [2006] JOL 17063 (SCA) This case was concerned with the copyright in a computer program known as Data Explorer. The Data Explorer program could interrogate and manipulate what is known as All Media Products Survey (AMPS) data. AMPS data are research results which are especially useful to marketing agencies in the planning of marketing strategies. The appellant developed a similar program named Brewer's AMPS which consisted of search and graphing functions. The source codes in Brewer's AMPS had been copied from the Data Explorer program. The High Court failed to differentiate between a computer program and a database and the SCA held that it erred in this regard as a database falls under the category of a literary work in the Copyright Act. The court upheld the appeal and found that the respondents' conduct amounted to copyright infringement of the Data Explorer computer program but insofar as improvements to the program and compilations characterised as databases were concerned, the respondents had satisfied the originality threshold and there was therefore no copyright infringement.

Board of Healthcare Funders v Discovery Health Medical Scheme and Others [2013] JOL 30806 (GNP) The applicant contended copyright infringement regarding a Practical Code Numbering System ("PCNS") which comprises of a set of numbers or codes which relate to and identify all of the medical practitioners and medical service providers in private practice in South Africa with related data. The applicant sought to protect the compilation insofar as it consists of the combination of a series of digits as well as the data of which it comprised which in its totality forms the PCNS. The respondents raised a number of defences including that no copyright existed in the work. The court rejected all of the respondents' contentions and found that the applicants had proved that the compilation and the work in its entirety was an original work and that they were the authors of the work. The court accordingly granted an order restraining the respondents from infringing the copyright and ordered the respondents to deliver to the applicant all databases, records and/or documents which incorporate the PCNS or any part, adaptations or infringing copies thereof in whatever storage medium they exist. The court confirmed that in deciding whether work in the nature of a compilation is original, the compilation should be considered in its entirety (not whether individual parts are original). The Court also confirmed that creativity is not required to make a work original: substantial work and energy in the compilation of the data could suffice. This case (and the *Haupt* one mentioned above) confirms the establishment of a low threshold for originality in South African law with regard to databases, which incorporates the 'sweat and brow' doctrine from UK law. This means that a database owner can enjoy copyright protection in both original and non-original databases.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

UPCOMING LEGISLATIVE CHANGES

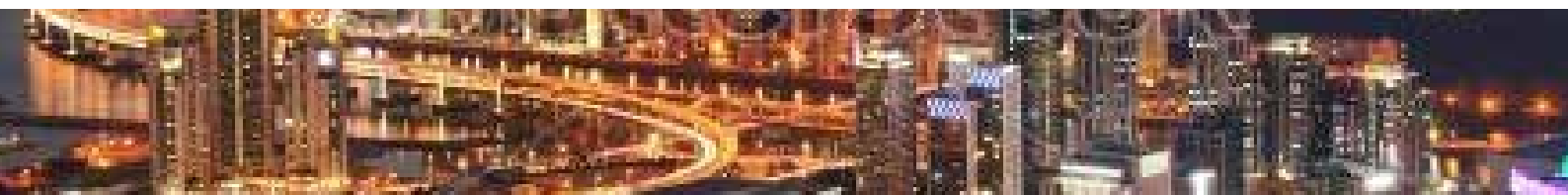
As noted above, the POPI Act has been assented to and will be effective on a date to be proclaimed. A one year transition period is provided for.

TOP TIP FOR DATABASE OWNERS

Establish strong protection rights through ensuring adequate contractual protections are in place or accepted by users prior to or at the time of accessing the database which should include licensing provisions, restraints on use and contractual requirements to return physical property on which the database is stored.

TOP TIP FOR THOSE LOOKING TO EXPLOIT BIG DATA

For those looking to exploit Big Data, the nature of the data is vital especially if it is personal information as defined in the POPI Act (including if it falls within the category of ‘sensitive’ or special information or information relating to children). Businesses looking to exploit Big Data must make sure they comply with the provisions of the POPI Act.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

17. SOUTH KOREA

KEY CONTACTS



Kwang Bae Park
T +82 2 772 4343
kwangbae.park@leeko.com



Hwan Kyoung Ko
T +82 2 2191 3057
khk@leeko.com

ORIGINAL DATABASES

Protected? A database which is creative in nature in terms of selection, arrangement, or composition of its subject matters may be protected in Korea as a ‘Compilation work’ under the Korean Copyright Act (Law No. 11903; amended 16 July 2013) (“**Copyright Act**”).

Ownership The database author(s) are the first owner(s) of the copyright, unless made as a work-for-hire within the scope of the author’s employment (in which case the employer is the first owner if the work is made public under the name of such employer).

Pre-conditions A database must be “original”. It must have ‘a creative nature’ in terms of selection, arrangement, or composition of its subject matter. In addition, the database must be fixed in a tangible medium of expression (e.g. written down or stored on a disk). However, copyright does not protect the underlying data (i.e. facts or base information). It is not required to register the copyright. However, if copyright is registered on the copyright register maintained by the Minister of Culture, Sports and Tourism, the person whose name is registered shall be presumed to be the author of the registered work and the registered date of creation or having first been made public shall be presumed to have been created or first made public on the date registered. In addition, any person who infringes the registered copyrights shall be presumed to have been negligent in his act of infringement.

May cover Databases with a complex structure (i.e. non-obvious format/choice of data types) based on an assessment of customer/business needs.

Unlikely to cover Databases which are structured in an obvious way and/or produced by an automated computer process.

Duration Copyright protection lasts for the author’s life plus 70 years after the end of the calendar year in which the author (or the last author, if the database is a work of joint authorship) dies.

Scope of Protection Copyright is infringed by doing acts proscribed in Korean copyright law (e.g. reproducing the database, performing the database publicly, communicating the database publicly, exhibiting the original or copies of the database, distributing the original or copies of the database, producing and exploiting a derivative work based on the database) by a third party without authorisation of the copyright owner.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Remedies include Injunctions and/or damages in case of civil liability. In instances of intentional infringement, criminal sanctions are possible, including imprisonment of up to five years or a criminal fine.

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Protected? The database of a person who is a Korean national or a foreigner protected by treaties that the Republic of Korea has acceded to or ratified in connection with a database protection regime shall be protected even without the proof of originality under Chapter Four of Korean Copyright Act (Article 91-98).

Ownership A database producer shall retain the rights. Database producer shall mean the person who made a substantial investment in human or material resources to produce the database, or renewal, verification, or its subject matters (Article 2, Item 20 of the Copyright Act).

Pre-conditions A substantial investment should be made by a producer in human or material resources in producing the database, or renewal, verification of its subject matter.

May cover Marketing databases, record of live actions occurring during a sporting event, and case law databases (i.e. a substantial investment was made).

Unlikely to cover A list of runners and riders in a horse race (i.e. a substantial investment has not been made).

Duration The right arises upon creation of the database and lasts for 5 years from the year subsequent to the year of its creation. When substantial updates or changes are made to the database, a new 5 year period right commences from the year following the year of its creation.

Scope of protection A database producer can prevent any unauthorized third party from reproducing, distributing, broadcasting, or interactive transmission of all or a substantial part of the database.

Remedies include Injunctions and/or damages in case of civil liability. In instances of intentional infringement, criminal sanctions are possible, including imprisonment of up to five years or a criminal fine.

CONFIDENTIAL DATABASES

Protected? Confidential databases can be protected by various laws including but not limited to the South Korean Unfair Competition Prevention and Trade Secret Protection Act, Civil Law and/or Criminal Law provided that certain requirements for protection under each law (e.g. trade secrecy of Unfair Competition Prevention and Trade Secret Protection Act) are satisfied. However there is no specific law for protecting confidential databases in South Korea.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

PERSONAL DATA

Is personal data given particular protection? Personal data is protected in South Korea under the Personal Information Protection Act (“**PIPA**”), a general law. Depending on the nature and/or type of personal data, the information may also be protected under special laws such as the Act on Promotion of Information and Communications Network Utilization and Information Protection (“**ICNA**”) and the Use and Protection of Credit Information Act (“**UPCIA**”).

South Korea’s privacy laws impose stricter regulations compared to those of other countries and the authorities responsible for enforcing these laws also show little leniency in imposing heavy criminal penalties and administrative fines on violators.

Of particular note is the massive security breach of three major credit card companies that occurred in January 2014, which in turn prompted the regulatory authorities to strengthen their oversight and enforcement of personal data regulations and gear up to amend privacy laws such as the PIPA.

Who can rely on it? Any living individual can take advantage of the protections offered by the PIPA, although the same does not hold true for the special laws. The ICNA only applies to users of information and communication services, while the UPCIA only applies to data subjects of credit information.

What data? The concept of personal data under South Korean law is extremely broad, and refers to any data relating to a living natural person from which the individual can be identified (including any information from which, if not by itself, but as easily combined with any other information, a specific individual is identifiable). In recent rulings by the lower-level Korean courts, even the IMEI numbers and last four digits (out of 11 total) of mobile phone numbers have been found to be personal data.

Scope of protection The legislation provides detailed regulations on the processing (e.g. collection, storage, access, use, transfer) of personal information. This can limit what the owner of a database can legitimately do with that database (particularly marketing databases).

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

In principle, the handling of resident registration numbers (RRNs) is prohibited under South Korean law, while personal data obtained by financial institutions (e.g. banks) is subject to stricter rules.

SIGNIFICANT RECENT CASES

Decision of the Supreme Court (April 24, 2014; 2014Do239): The court ruled that because it has become more and more common in Korea (where subscribers are allowed to choose the last four digits of their cell phone numbers) for mobile phone users to select a four-digit sequence that has personal meaning or significance to oneself, the last four digits of mobile phone numbers also constitute personal data by which an individual could be identified (e.g. because all cell phone numbers in Korea start with 01, and typically take the format of 01X-XXXX-XXXX, subscribers tend to use the last four digits of their home phone number or pick a sequence that is consistent with the mobile phone number of a family member).



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

KCC's imposition of a KRW 212.3 million fine on Google Inc.: On January 28, 2014, the Korea Communications Commission (“KCC”), the regulatory agency responsible for enforcing the ICNA, fined Google Inc. KRW 212.3 million for collecting unencrypted personal information of users (e.g. IDs, passwords, RRNs, Mac Addresses) exchanged over WiFi networks without obtaining the prior consent of the users in developing Google’s Street View Services. The KCC also ordered Google Inc. to delete all personal data that it had collected in this manner and to disclose the deletion process to the KCC.

UPCOMING LEGISLATIVE CHANGES

1. Due to the largest-ever data breach that occurred in January, regulators are expected to strengthen enforcement of the relevant laws (e.g. the UPCIA) and amend them so that stronger measures are put in place for the protection of personal data. The amended version of the ICNA is set to take effect on November 29, 2014. The amended ICNA stipulates, among other things, statutory damages for users affected by a data breach and an explicit 24-hour deadline for reporting a data breach. Therefore, any database owners intending to process the personal information of Koreans in the future are recommended to keep tabs on any legislative updates and changes in the regulating authorities’ positions on the matter.
2. At the end of 2013, the KCC announced a draft version of the “Big Data & Personal Information Protection Guidelines,” and although the Guidelines have not yet been officially adopted, it would be helpful for anyone who wishes to exploit big data in Korea to review the provisions and make note of any subsequent developments relating to the Guidelines.

TOP TIP FOR DATABASE OWNERS

There is no requirement to register the copyrights or the rights of database producers. However, if such rights are registered on the copyright register maintained by the Minister of Culture, Sports and Tourism, any person who infringes upon the registered copyrights or rights of the database producers shall be presumed to have been negligent in his act of infringement. It is recommended that you register your copyrights or rights of database producers on the copyright register.

TOP TIP FOR THOSE LOOKING TO EXPLOIT BIG DATA

Because Korea imposes very strict regulations on the handling of personal information, the biggest issue with respect to the big data business in Korea also pertains to personal data protection. As such, those looking to exploit big data should be well-versed in the specific privacy and data protection regulations so that their business (involving the exploitation of big data) is not found to be in violation of any applicable statutes.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

18. SPAIN

KEY CONTACTS



Diego Ramos
Partner
T +34 91 790 1658
diego.ramos@dlapiper.com

The law is part harmonised with general EU law (see [EU section](#)). In this section we therefore only highlight areas that differ from EU wide law.

ORIGINAL DATABASES

Spain is subject to the EU-wide Database Directive (see [EU section](#)), implemented by the 1996 [Spanish Intellectual Property Act \(SIPA\)](#) (link is to Spanish-language version), and expected to change in the summer of 2014). Article 12.2 of the SIPA defines “database”. SIPA is applicable all over the territory of Spain. Such copyright protection would be independent from copyright in the individual items forming part of the database.

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

The EU-wide Database Directive (see [EU section](#)) applies and was implemented by [SIPA](#), Article 133.1 of which provides for the database right.

CONFIDENTIAL DATABASES

There is no general civil right in Spain to prevent misappropriation of confidential information, other than where a contractual obligation of confidentiality has been agreed. The Spanish Criminal Code prohibits (in articles 278 and 279) the misappropriation and disclosure of business secrets (and more broadly, any type of private/reserved information in article 197). However, the Spanish criminal courts will normally not enforce these provisions (except for article 197), other than where there is a very carefully drafted contractual obligation of confidentiality in place, which qualifies the information as “valuable trade secrets”.

PERSONAL DATA

See [EU section](#) above. The handling of “personal data” is subject to the [Spanish Data Protection Act 1999](#) (link is to English translation). As a peculiarity of the Spanish system, lack of compliance with data protection law is aggressively prosecuted by the authorities, in most cases through hefty financial penalties.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

Generally, no. Personal information databases owned by the State and other public bodies enjoy special rules within the Spanish Data Protection Act 1999, especially regarding creation, registration and enforcement, but otherwise follow the general rules.

SIGNIFICANT RECENT CASES

There has been only very limited recent case law in Spain on the protection of databases.

In relation to (personal) data protection, in *Saberlotodo.com* the leading portal supplying personal information to the financial services and debt recovery sectors was fined €5 million in 2011, after the Spanish Data Protection Commissioner found that it had built up personal information databases using data that could be handled only with the informed prior consent of the data subjects. The database owner was also found to have resisted the investigations launched by the Commissioner and provided incomplete information to investigators.

UPCOMING LEGISLATIVE CHANGES

Nothing at a national level (see [EU section](#) above). Current discussions for the amendment of SIPA should in principle not entail any major modification of the framework for databases in Spain, although this could change once the draft legislation is finally agreed.

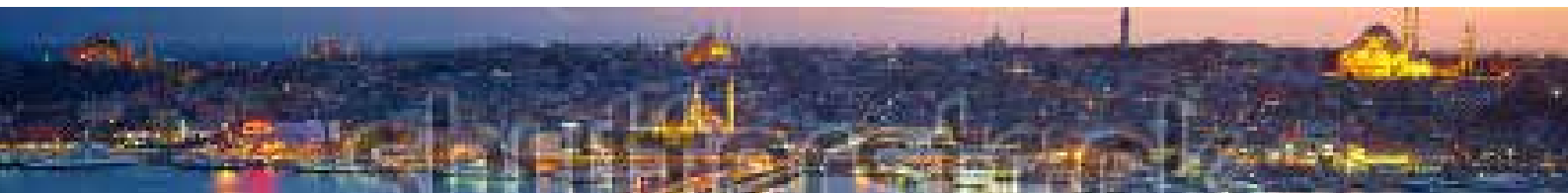
TOP TIP FOR DATABASE OWNERS

To maximise your chances of being able to establish rights over your database:

1. make filings of the database structure and contents from time to time with Notaries Public.
2. make sure that the contracts with employees and external contractors clearly state that both the copyright and database right derived from SIPA are vested in you.
3. make any disclosure of confidential data subject to prior signature of an appropriate NDA, bearing in mind the relative lack of non contractual protection of confidential information in Spain.

TOP TIP FOR BIG DATA OWNERS

Verify that proper and informed consent has been obtained from data subjects in connection to the combination of databases, the enhancement of databases and the use of data for additional/alternative purposes, typical of Big Data.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

19. TURKEY

KEY CONTACTS



Gökhan Gökçe
Partner
T +90 212 318 0508
ggokce@
yuksekkarkinkucuk.av.tr



Burak Ozdagistanli
Associate
T +090 212 318 05 16
bozdagistanli@
yuksekkarkinkucuk.av.tr

ORIGINAL DATABASES

Protected? Pursuant to Art. 6 paragraph 11 of the Turkish Law on Protection of IP Rights, original databases are protected as “compiled work” or works created through compiling works. (An English translation can be found at [here](#)).

Ownership Copyright in the database vests with the compiler or author of the database.

Pre conditions Database must be “original” in selection or arrangement of the data in the database. Further, it is accepted that the personality of the author must be reflected in the database. Also, database must be accessible via separate tools or other ways. Registration is not required, as soon as the database is formed, it gains protection.

May cover Marketing databases with a personal touch by the author.

Unlikely to cover Standard databases with no originality such as a train schedule for the upcoming week.

Duration Copyright protection lasts for the duration of the author’s life plus 70 years after death (this applies to the last author in instances of joint authorship). However, if the first author is a legal person, protection is limited to 70 years from publication of the database.

Scope of protection A database has the same level of protection as an artistic work (a book, painting etc.) under Turkish Law. Therefore database owners have a right to prevent others making copies of the database or making the database available to the public. Further, they can also prevent other people altering, adapting, translating, copying or leasing out the database without their permission.

Remedies Infringement of copyright will result in civil and criminal liability. In respect of civil liability, the author may request up to 3 times the value of the database together with injunctions to prevent infringement.

In respect of criminal liability, the infringer is subject to 1 to 5 years of imprisonment or a judicial fine.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Protected Databases in which an investment has been made are protected pursuant to Additional Art. 9 Paragraph 4 of the Law on Protection of IP Rights.

Ownership Copyright and the right of protection in the database vests in the investor.

May cover Marketing databases with a personal touch by the author.

Unlikely to cover Standard databases with no originality such as a train schedule for the upcoming week.

Duration Protection for databases in which an investment has been made lasts 15 years.

CONFIDENTIAL DATABASES

Protected? In addition to the copyright protection, confidential databases may be protected as commercial secrets under the Turkish Commercial Code (“TCC”) in terms of unfair competition rules.

Owner TCC protects the owner of the database.

Pre-conditions Owner must take reasonable care to keep the database confidential.

May cover Any database which may be understood as a trade secret or information specific to the owner.

Unlikely to cover Databases consisting of readily available information.

Duration Protection arises when the database (which the owner has made efforts to keep confidential) is created and will last until publication by the owner or an authorised party.

Scope of protection Unauthorised acts include the unauthorised publishing or use of the confidential database.

Remedies A company may recover compensation for loss suffered from a breach and may obtain injunctions to prevent intended publication, where this has not already occurred.

PERSONAL DATA

Is personal data given particular protection? As yet, Turkey does not have a specific data protection law in respect of personal data. Therefore protection of personal data is subject to The Constitution of the Turkish Republic, Turkish Criminal Code and the Turkish Code of Obligations.

Who can rely on it Data subjects (individuals).

What data? There is no specific definition of personal data. However it is accepted that the definition of personal data is in line with the EC Directive 95/46.

Scope of protection Not specifically identified.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

Personal data obtained by institutions that are subject to Banking Law and insurance companies is subject to stricter rules, requiring such institutions to protect their clients' financial data.

SIGNIFICANT RECENT CASES

Legal regime in Turkey is not based on case-law precedents and cases are not publicly available.

UPCOMING LEGISLATIVE CHANGES

The Draft Law on Data Protection has been pending for some time and is expected to be enacted in 2014. The Draft Law is in line with the EC Directive 95/46.

TOP TIP FOR DATABASE OWNERS

Identification of the author is very important for protection of databases. Therefore records identifying the author and history of the database must be kept carefully.

TOP TIP FOR THOSE LOOKING TO EXPLOIT BIG DATA

Exploiting big data will involve processing and maybe transferring data collected previously. Therefore we advise clients to make sure that appropriate consent is obtained for processing/transferring personal data.



- Australia
- Austria
- Belgium
- Brazil
- China
- EU
- France
- Germany
- Hong Kong
- India
- Italy
- Japan
- The Netherlands
- Romania
- Singapore
- South Africa
- South Korea
- Spain
- Turkey
- UK
- USA

20. UK

KEY CONTACTS



John Wilks
 Partner
 T +44 (0)20 7796 6288
 john.wilks@dlapiper.com



Catherine Beloff
 Senior Associate
 T +44 (0)20 7796 6190
 catherine.beloff@dlapiper.com



Simon Levine
 Partner
 T +44 (0)20 7796 6020
 simon.levine@dlapiper.com



Jim McDonnell
 Senior Associate
 T +44 (0)114 283 3395
 jim.mcdonnell@dlapiper.com



Ruth Hoy
 Partner
 T +44 (0)20 7796 6457
 ruth.hoy@dlapiper.com

The law is part harmonised with general EU-law (see [EU section](#)), in this section we therefore only highlight areas that differ from EU-wide law.

ORIGINAL DATABASES

See [EU section](#). Under English case law the infringing acts can be undertaken in relation to a substantial part (measured qualitatively), or the whole of the database. This must now be read in the light of CJEU case law which expressed the relevant test as whether the part reproduced expresses “the intellectual creation of the author”²⁸

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

Subject to EU wide Database Directive (see [EU section](#)), implemented by the [UK Copyright and Rights in Databases Regulations 1997](#).

²⁸ See *Infopaq*.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

CONFIDENTIAL DATABASES

Protected? It is possible for confidential databases to be protected under the law of confidence. The equitable action for breach of confidence does not protect the information per se, but rather the unconscionable use or threatened use of such information when it is imparted in circumstances of confidence. See eg. *Coco v AN Clark (Engineers) Ltd*²⁹, which is national law.

Ownership The protection of confidence may cover the confider of the database, but only in circumstances where the recipient of the information owes the confider an obligation to keep the information confidential (i.e. if a reasonable person in the position of the recipient would understand that the information was given in confidence).

Pre-conditions The information contained in the database will not be protected under the law of confidential information unless:

- (i) the information has the necessary quality of confidence;
- (ii) the owner has taken sufficient steps to preserve the confidentiality of its information; and
- (iii) a reasonable person in the position of the recipient would understand that the information was given in confidence.

May cover Customer databases, databases of a company's commercial or technical knowhow, databases of product ingredients.

Unlikely to cover Data that is published or licensed on terms which do not impose confidentiality obligations.

Duration Protection arises from the time the obligation of confidence arises (providing the confidential database) and lasts until the obligation ceases (usually until information passes into the public domain).

Scope of protection Usual elements to establish breach of confidence are (in addition to those listed above) that:

- (i) the information must have been imparted in circumstances importing an obligation of confidence; and
- (ii) there must be an unauthorised use (or threatened unauthorised use of that information to the detriment of the party communicating it).

Remedies Injunctions (interim and final), damages or an account of profits, delivery up or destruction, payment of legal costs.

PERSONAL DATA

See [EU law section](#). The EU wide Data Protection Directive is implemented in the UK by the [Data Protection Act 1998](#). The UK regulator, the ICO, issued guidance on Big Data and Data Protection on 28 July 2014; see [here](#).

²⁹ [1969] RPC 41



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

No.

SIGNIFICANT RECENT CASES

Football Dataco v Sportradar: the English Court of Appeal held that that a database of data relating to match events such as goals and bookings collected live during football matches was protected by database right. The Court reasoned that such data was created when the event happened (e.g. when the referee declared a goal had been scored), not when it was recorded in the database. The database included some “subjective” data items which had been “created” by the database owner (e.g. selection of the best player of the match). But because it also included “objective” data items which had been merely obtained by the database owner (e.g. goals, times, scorers), it was protected by database right. The right was infringed in the UK through extraction of data:

- by UK-based individuals who download the data onto their computers;
- by the German data supplier, through both (i) communicating the data to the public via a pop-up box accessible from its client’s websites, and (ii) being jointly liable with the individuals; and
- by the Gibraltar-based client which owned the website from which the pop-up box was accessed, through being jointly liable with the individuals.

BSkyB v Digital Satellite Warranty Cover: the English High Court held that database right subsisted in BSkyB’s database of customer details, rejecting an argument that because the details were entered by BSkyB the contents of the database were “created” by .BSkyB.

UPCOMING LEGISLATIVE CHANGES

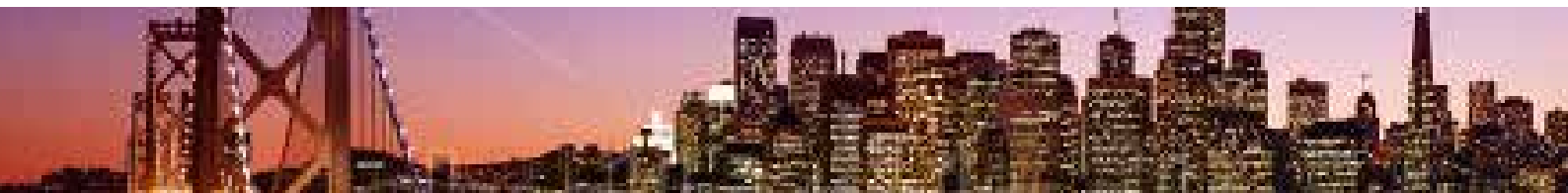
The UK government has just widened certain defences to copyright infringement. These include a new defence to allow text and data mining for non-commercial research, which came into force on 1 June 2014.

TOP TIP FOR DATABASE OWNERS

Audit the data you own: consider the range of potential rights available to protect the data in the UK, and take steps to ensure you benefit from such protection, such as obtaining written IP assignments from all those who could potentially own the rights (note in particular that a UK contractor who creates a copyright-protected database is likely to own it in the absence of express contrary provision).

TOP TIP FOR THOSE WHO EXPLOIT BIG DATA

4. If exploiting data received from a third party, obtain contractual indemnifications to give protection in the event that data infringes another’s IP (this would for example have protected the data customer in the *Sportradar* case referred to above).



- Australia
- Austria
- Belgium
- Brazil
- China
- EU
- France
- Germany
- Hong Kong
- India
- Italy
- Japan
- The Netherlands
- Romania
- Singapore
- South Africa
- South Korea
- Spain
- Turkey
- UK
- USA

21. USA

KEY CONTACTS



Andrew Deutsch
 Partner
 T +1 212 335 4880
 andrew.deutsch@dlapiper.com



Jim Halpert
 Partner
 T +1 212 335 4880
 jim.halpert@dlapiper.com

ORIGINAL DATABASES

Protected? Databases are considered to be compilations under US copyright law; they may be protected by copyright if their selection and arrangement is creative, under the federal **Copyright Act**. However, the data within databases, if factual, may not be copyrighted as a matter of both US constitutional law (see *Feist Publications, Inc. v. Rural Telephone Service Co.*) and statutory copyright law (federal Copyright Act 17 U.S.C. § 102(b)).

Ownership Copyright belongs to the author of the database, or, where the database is created by an employee in the course of employment, the copyright belongs to the employer.

Pre-conditions Copyright protection arises upon creation of a copyrightable work, and registration is not needed. Registration is needed (for US origin works only) in order to bring an infringement suit. Registration prior to infringement (or within three months of first publication, if infringement occurs prior to publication) is required to enable the copyright owner to (i) elect to receive statutory damages if it prevails in an infringement suit, and (ii) be eligible for a discretionary award of attorneys' fees.

May cover Compilations of estimated values of used automobiles; systems for classifying diseases.

Unlikely to cover Telephone directories organized alphabetically; lists of sequentially numbered machine parts.

Duration The right arises upon creation. For works created since 1978, US copyright law gives a copyright term of the life of the author plus 70 years.

Scope of protection Copyright is infringed through unauthorized reproduction, distribution, or display of the original work, or preparation of a derivative work from the original work, which takes non-de minimis copyrightable elements of the original (e.g., the selection or arrangement of otherwise non-copyrightable facts), so that there is substantial similarity between those copyrightable elements and the infringer's work.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

Remedies include (i) damages; (ii) infringer's profits, to the extent not considered in the calculation of damages; (iii) if the copyright holder has timely registered its work, and at its election, it may recover, instead of actual damages and profits, statutory damages in the discretion of the court, which may range from US\$750 to US\$30,000 per infringed work for ordinary infringements, or up to US\$150,000 for willful infringements; (iv) if the copyright holder has timely registered its work, the costs of the action, including a reasonable attorney's fee, in an amount to be determined by the court.

DATABASES IN WHICH AN INVESTMENT HAS BEEN MADE

There is no additional protection – copyright protection for selection, and arrangement is not dependent upon whether investment has been made.

CONFIDENTIAL DATABASES

Protected? Most states have adopted the **Uniform Trade Secrets Act**, which defines confidential information subject to protection, and databases may fall under it. State common law may impose a duty on employees and others in a position of confidence to refrain from copying or disclosing confidential information. State contract law may also provide protection against copying databases by contract signatories. The courts have distinguished between negotiated contracts and “clickwrap” agreements (under which clicking a link is intended to constitute agreement to non-disclosure terms). Some courts have been reluctant to enforce the latter, particularly where there were questions as to whether a user was aware of and assented to restrictions.

Ownership. In common law cases of duty not to disclose, protection will be granted to the employer or party disclosing in confidence. Protection belongs to the creator of the database in contract cases.

Pre-conditions. In cases of common-law duties not to disclose, while there is some variation in state law, the requisites are usually (i) that the information is not generally known, (ii) the owner of the database has taken reasonable measures to protect the confidentiality of the information, and (iii) that the party receiving the database is an employee or is otherwise under an implied legal duty to protect the confidentiality of the information. In contract cases, the terms of the contract determine the position, and must clearly establish an intention that the party bound by the contract will not copy from the database or disclose its contents except as provided by the terms.

May cover. Customer lists; commercial or technical knowhow, product formulations; software and informational tables.

Duration. In cases of common-law duties not to disclose, protection arises upon the disclosure of the information to the person bound by the duty, and is perpetual, unless the information enters the public domain without involvement of the party to whom it is disclosed, or is published by the owner. In contract cases, protection arises upon disclosure and lasts for



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

the period stated in the contract. In non-disclosure agreements, the obligation to maintain information as confidential continues after the term of the agreement, until the information enters the public domain or is published by the owner without a restriction on further dissemination or use.

Scope of Protection Contract. Cases will vary according to the terms of the contract, however, typically, infringement occurs upon disclosure to an unauthorised person, unauthorised publication, or upon use in violation of the terms of the agreement. The same scope of protection is generally imposed in cases where a common-law duty not to disclose is found.

Remedies. Preliminary and permanent injunctive relief, and compensatory damages measured by the economic injury to the party owning the database. There is potential for award of punitive or exemplary damages in common-law duty cases where the confidential information is willfully used in disregard of the rights of the owner. Punitive and exemplary damages are not awarded in contractual cases.

PERSONAL DATA

Is personal data given particular protection? There is a variety of laws and regulations at national and state levels protecting personal data.

Who can rely on it? Data subjects and national and state consumer protection authorities can assert these rights.

What data?

1. personal health data
2. personal information presented in credit reports and other reports hearing on a data subject's reputation
3. non-public personal data compiled by a financial institution
4. educational records regarding students and in some states other student information collected by educational contractors
5. data regarding subscribers to communications services or video services
6. taxpayer data
7. data collected online from children; and a variety of other specific contexts
8. social security numbers and other government identification numbers.

Scope of protection. This will depend upon the type of data or industry regulated and any statement in an applicable privacy policy regarding use or disclosure of personal data. Typically this will include some combination of requirements of notice, consent, user access and correction of data and provisions requiring the data to be kept secure.



Australia
Austria
Belgium
Brazil
China
EU
France
Germany
Hong Kong
India
Italy
Japan
The Netherlands
Romania
Singapore
South Africa
South Korea
Spain
Turkey
UK
USA

ANY OTHER FORMS OF PROTECTION FOR PARTICULAR TYPES OF DATA?

Databases created by employees of the US Government are not entitled to copyright protection, under section 105 of the federal [Copyright Act](#). Databases created by state or local governments, in contrast, may be protected by copyright.

SIGNIFICANT RECENT CASES

Feist Publications v. Rural Telephone Service Co. in which the US Supreme Court held, as a matter of constitutional law, that copyright law cannot protect the contents of databases against extraction and copying, but may provide a “thin” copyright for the original selection and arrangement of the data.

Bellsouth Advertising and Publishing Corp. v. Donnelley Information Publishing, Inc. in which the 11th Circuit of the US Court of Appeals held that classification and factual information from “yellow pages” directories are not protected by copyright and may be freely copied.

UPCOMING LEGISLATIVE CHANGES

None currently – a number of bills that would have created a sui generis protection were considered but not enacted.

TOP TIP FOR DATABASE OWNERS

Where at all possible, establish strong protection rights through individually negotiated contracts. If databases are made available to a mass market and negotiation is not possible, make sure that contractual provisions against disclosure/dissemination are visible to the user and that the user’s assent to those conditions can be clearly evidenced. Also consider (particularly in the case of sophisticated corporate users) whether to make contractual rights in the database subject to the laws of a country with stronger database protection than the US, if either the provider or user has some connection to that country. US courts will frequently enforce a choice of foreign law among sophisticated parties, even though due process may require the use of a US forum to enforce those rights.

TOP TIP FOR THOSE WHO EXPLOIT BIG DATA

Ensure that you have the contractual right to use the data in the manner you intend, that you are not precluded from doing so by a data privacy restriction, and whether you may be able to use the data by de-identifying it.



If you have finished with this document, please pass it on to other interested parties or recycle it, thank you.

www.dlapiper.com

This handbook is provided to you as a courtesy, and it does not establish a client relationship between **DLA Piper** and you, or any other person or entity that receives it. It provides a general overview of the law governing rights in data/databases currently in force in 20 jurisdictions. It is a general reference document and should not be relied upon as legal advice. The application and effect of any law or regulation upon a particular situation can vary depending upon the specific facts and circumstances, and so you should consult with a lawyer regarding the impact of any of these regimes in any particular instance. **DLA Piper** accepts no liability for errors or omissions appearing in the handbook. Please note that IP law is dynamic, and the legal regime in the countries surveyed could change. No part of this publication may be reproduced or transmitted in any form without the prior consent of the **DLA Piper**.

Copyright © 2014 DLA Piper. All rights reserved. | SEP14 | 2814242