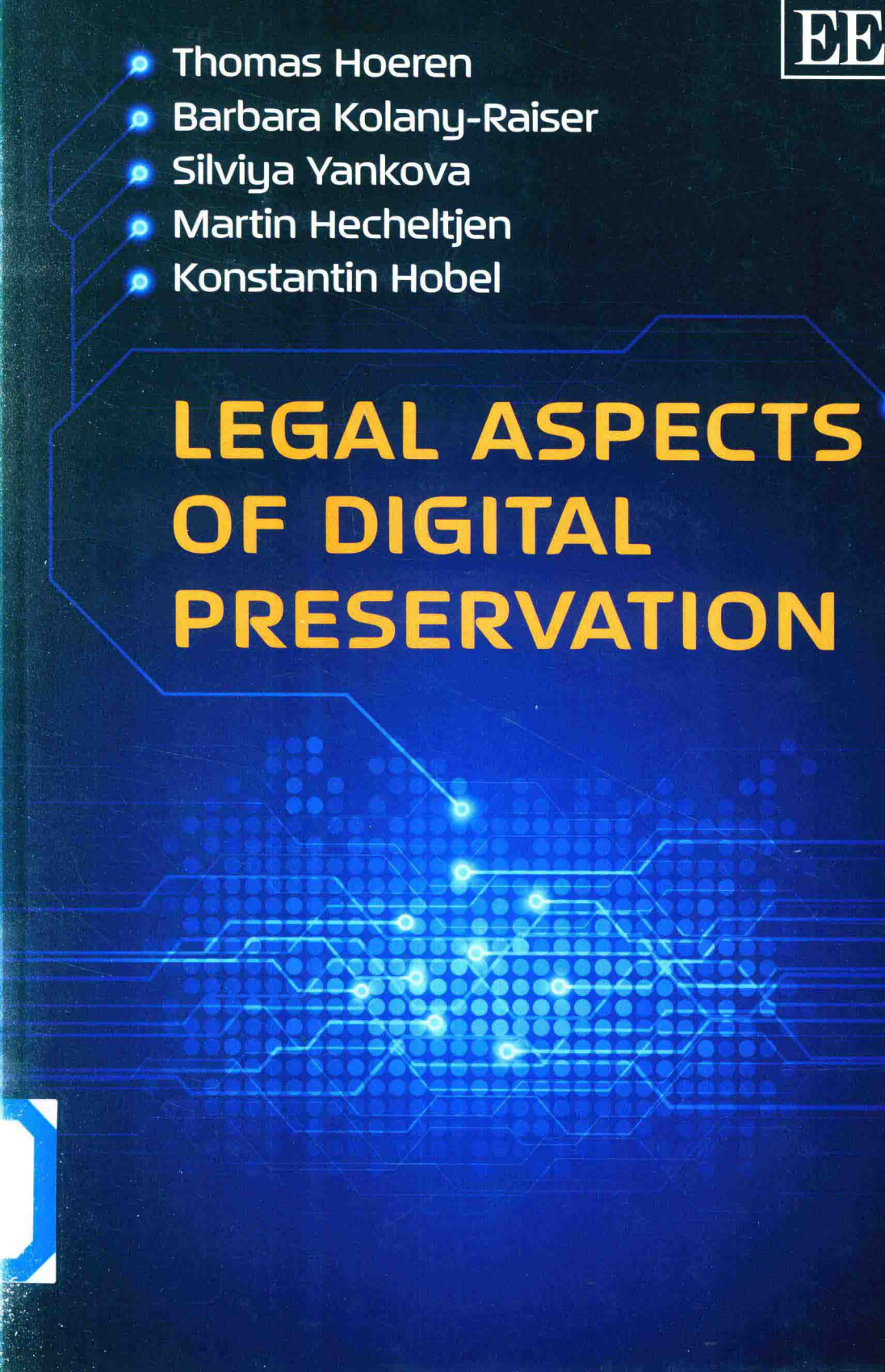
Thomas Hoeren
Barbara Kolany-Raiser
Silviya Yankova
Martin Hecheltjen
Konstantin Hobel

LEGAL ASPECTS OF DIGITAL PRESERVATION



Legal Aspects of Digital Preservation

Thomas Hoeren

Institute for Information, Telecommunication and Media Law, Germany

Barbara Kolany-Raiser

Institute for Information, Telecommunication and Media Law, Germany

Silviya Yankova

Institute for Information, Telecommunication and Media Law, Germany

Martin Hecheltjen

Institute for Information, Telecommunication and Media Law, Germany

Konstantin Hobel

Secure Business Austria

Edward Elgar

Cheltenham, UK • Northampton, MA, USA

Published by
Edward Elgar Publishing Limited
The Lypiatts
15 Lansdown Road
Cheltenham
Glos GL50 2JA
UK

Edward Elgar Publishing, Inc.
William Pratt House
9 Dewey Court
Northampton
Massachusetts 01060
USA

A catalogue record for this book
is available from the British Library

Library of Congress Control Number: 2013931294

This book is available electronically in the ElgarOnline.com Law Subject Collection, E-ISBN 978 1 78254 666 5

ISBN 978 1 78254 665 8

Typeset by Columns Design XML Ltd, Reading
Printed and bound in Great Britain by T.J. International Ltd, Padstow

Legal Aspects of Digital Preservation

Acknowledgements

The authors wish to acknowledge the valuable contributions from the following contributors:

DI Mark Guttenbrunner, Verein zur Förderung der IT-Sicherheit in Österreich (SBA)

DI Mag. Stephan Strodl, Verein zur Förderung der IT-Sicherheit in Österreich (SBA)

Stefan Pröll, MSc, Verein zur Förderung der IT-Sicherheit in Österreich (SBA)

Dr Daniel Simon, Software Quality Systems AG (SQS)

Daniel Draws, Software Quality Systems AG (SQS)

The authors would also like to thank Gregor Heinrich from iPharro Media GmbH and Phil Mondor from Intel Corporation for their assistance in reviewing the text and their helpful suggestions; and Jackie Bronsdon, Shalene Edwards, Hauke Gärtner, Paul Strakeljahn, Jan Brandenburg and Michael Thiesen for their valuable research assistance.

This volume was produced as a part of the TIMBUS project (Timeless Business Processes and Services). TIMBUS is a three-year collaborative project co-funded by the European Commission under the Seventh Framework Programme for research and technological development and demonstration activities (FP7/2007). However, the views and opinions expressed in this book reflect only the authors' point of view and not necessarily those of all members of the TIMBUS project or the European Commission.

Abbreviations

AG	Aktiengesellschaft, corporation/public company
AMC	acceptable means of compliance
BCR	binding corporate rule
BGBl	Bundesgesetzblatt, Federal Law Gazette (Austria)
BGH	Bundesgerichtshof, Federal Court of Justice (Germany)
CAMO	Continued Airworthiness Management Organization
CEN	European Committee for Standardization
EASA	European Aviation Safety Agency
ECHA	European Chemicals Agency
ECJ	European Court of Justice
EDI	electronic data interchange
EMI	European Medicines Agency
EU	European Union
EUPL	EU public licence
FAQ	frequently asked question
FLAC	Free Lossless Audio Codec
GCP	good clinical practice
GmbH	Gesellschaft mit beschränkter Haftung, private limited company
GMP	good manufacturing practice
IPR	intellectual property right
MTTR	mean time to restore
OJ	Official Journal
OSS	Open Source Software
PJCCM	police and judicial cooperation in criminal matters
POA	production organization approval
SLA	service level agreement
TEU	Treaty on European Union

TFEU	Treaty on the Functioning of the European Union
VAT	value added tax

Austrian and German Statutes

ABGB	Allgemeines bürgerliches Gesetzbuch, Civil Code (Austria)
atAktG	Aktiengesetz, Stock Corporation Act (Austria)
deAktG	Aktiengesetz, Stock Corporation Act (Germany)
AngG	Angestelltengesetz, Employee Act (Austria)
AO	Abgabenordnung, Tax Code (Germany)
ArbVG	Arbeitsverfassungsgesetz, Labour Constitution Act (Austria)
ÄrzteG	Ärztegesetz, Act on the Medical Profession (Austria)
AVRAG	Arbeitsvertragsrechts-Anpassungsgesetz, Act amending the Labour Contract Law (Austria)
BAO	Bundesabgabenordnung, Federal Tax Code (Austria)
BDSG	Bundesdatenschutzgesetz, Federal Data Protection Act (Germany)
DSG	Datenschutzgesetz, Data Protection Act (Austria)
EStG	Einkommensteuergesetz, Income Tax Act (Austria)
FinStrG	Finanzstrafgesetz, Act on Financial Crime (Austria)
atGmbHG	Gesetz über Gesellschaften mit beschränkter Haftung, Limited Liability Companies Act (Austria)
deGmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung, Limited Liability Companies Act (Germany)
HGB	Handelsgesetzbuch, Commercial Code (Germany)
aIO	Insolvenzordnung, Bankruptcy Act (Austria)
gIO	Insolvenzordnung, Bankruptcy Act (Germany)
KAKug	Krankenanstalten- und Kuranstaltengesetz, Hospital and Sanatorium Act (Austria)

KStG	Körperschaftsteuergesetz, Corporate Tax Act (Austria)
SigG	Signaturgesetz, Signature Act (Austria)
atStGB	Strafgesetzbuch, Penal Code (Austria)
deStGB	Strafgesetzbuch, Penal Code (Germany)
StPO	Strafprozessordnung, Code of Criminal Procedure (Austria)
TKG	Telekommunikationsgesetz, Telecommunications Act (Germany)
UGB	Unternehmensgesetzbuch, Commercial Code (Austria)
UrhG	Urheberrechtsgesetz, Copyright Act (Germany)
atUStG	Umsatzsteuergesetz, Value Added Tax Act (Austria)
deUStG	Umsatzsteuergesetz, Value Added Tax Act (Germany)
UWG	Gesetz gegen den unlauteren Wettbewerb, Act Against Unfair Competition (Germany)
VAG	Versicherungsaufsichtsgesetz, Insurance Supervision Act (Germany)
VbVG	Verbandsverantwortlichkeitsgesetz, Corporate Criminal Liability Act (Austria)
atZPO	Zivilprozessordnung, Code of Civil Procedure (Austria)
deZPO	Zivilprozessordnung, Code of Civil Procedure (Germany)

Foreword

Our society has eagerly embraced the move from traditional information storage and processing, mostly on paper, to digital. We all benefit greatly from the increased functionality it provides us. Valuable scientific and cultural information assets are created, stored, managed and accessed digitally. In addition to data and document assets, we even encode scientific, business and manufacturing processes in digital form.

The threat of losing digital assets is high. Digital media are vulnerable: they decay and are short-lived. Over time, changes in the external environment pose additional risks. Data carriers become obsolete; software and hardware technologies required to access them fall into obsolescence; formats that are used to represent digital objects fall into disuse; 'representation information' that specifies how to access or interpret them is lost; and changes in organizations' cultural and financial priorities add risk. Unlike print-based materials, digital assets cannot survive significant gaps in care. In addition, if insufficient care is taken, any data and information management activity, such as when digital objects are copied, moved, renamed or reformatted, poses threats: digital assets may be damaged and knowledge about their origin may be lost, as well as knowledge about the historic relationships between renamed or versioned files. Loss of digital assets on a large scale has had an enormous economic and cultural impact on individual organizations and on cultural institutions.

These threats need to be addressed proactively through information management as well as digital preservation actions. Digital preservation 'combines policies, strategies and actions that ensure access to digital content over time' (Preservation and Reformatting Section (PARS), *Definitions of Digital Preservation*, American Library Association, Washington, DC, 2007, available at www.ala.org/ala/mgrps/divs/alcts/resources/preserv/defdigpres0408.pdf). Over the last two decades, the digital preservation community has focused efforts at creating technical and organizational solutions to this problem. Our responses to overcoming damage to data carriers and to the bits encoded on them include bit preservation through storage medium refresh and replication on several data carriers. Files in obsolete file formats or software on

outdated computing platforms can be migrated to better supported formats and platforms. Alternatively, obsolete systems can be emulated on newer platforms so that the original files or software can now be rendered or executed in a contemporary environment. Computer museums provide the means of authentic performance of digital assets on equipment for which they were designed. Digital forensic methods and recovery and reconstruction of lost and damaged files can be applied when loss has already happened. And finally, it is important to collect metadata which enables us to understand and use digital assets in the future.

Technical and organizational responses are critical, but they are limited by our ability to legally execute them. Legal aspects influence our ability to preserve documents, data, metadata and software. And they influence our ability to re-use them at an unspecified point in the future. This is complicated by the fact that regulations do not apply indefinitely and that circumstances change: for example, licences may expire, and legal regulations may change.

Legal Aspects of Digital Preservation addresses this very important problem. Rather than focusing on document and data preservation, some recent research projects have taken a more comprehensive look at the need to preserve whole rendering stacks and business execution environments. Examples are the KEEP project that investigated the digital preservation of software through its emulation on more modern platforms, and the TIMBUS project that is investigating the preservation of complete scientific or business processes. This touches on all aspects of the preservation challenge: business constraints; process descriptions; computational environments and their mutual dependencies; digital assets that are produced and consumed by the processes; roles of individuals and organizations; and dependencies on third party products and services. Both projects have rightly expended significant effort considering the legal implications of executing various digital preservation strategies in various use case scenarios in this larger scope. *Legal Aspects of Digital Preservation* adopts this comprehensive view. It should help legal practitioners and non-specialists to understand the legal issues to be considered in preparing digital preservation strategies, and is a very valuable contribution to the digital preservation discussion and practice at this time.

Dr Angela Dappert
Digital Preservation Coalition

Contents

1. Introduction

A substantial part of the information that we create and process in everyday life exists in digital form only. The major difference between such information, e.g. represented in data stored on a hard drive, and the information embodied in the text on the printed page of a book, is that the latter information is directly accessible for us as human beings.[1] In order to perceive the information represented in the digital object, however, we are in need of additional means. For the correct rendering of a book stored in the PDF format, for instance, it will first of all be necessary to be in possession of the right software. The execution of that software presupposes the corresponding operating system, which then in turn necessitates a certain hardware configuration to run properly.

Over time, all of these layers are prone to errors that can lead to the loss of data and thus information.[2] One reason for data loss is the obsolescence or destruction of data carriers or reader devices.[3] As technological progress in this area moves at a particularly rapid pace, another cause that can render the content of a digital object inaccessible is the obsolescence of the corresponding software or data format.[4] The loss of information represented in data might, moreover, occur despite of the availability of a functioning data carrier and reader device, when context that is needed to interpret the data properly is not (or no longer) available. In the case of text documents, the context information regarding the alphabet, text direction or character encoding used (e.g. Unicode) might not be available when trying to recover information from the document in the future. Encryption can constitute a further obstacle, if the decryption information is lost.[5]

---

[1] Cf. Borghoff, Rödig, Scheffczyk and Schmitz 2006: 489.

[2] For an introduction to the threats to the preservation of digital objects see Kuny 1998: 8–13.

[3] E.g. the example of the BBC's problems with the recovery/loss of data stored on contemporarily obsolete videodisk technology in the course of the Domesday Book project. For more detail see Charlesworth 2012: 19.

[4] Becker and Rauber 2007.

[5] Risak 2003: 238.

The first of the two most promising approaches towards keeping electronically stored information safe for the future is being referred to as *migration*, which can be defined as: 'A means of overcoming technological obsolescence by transferring digital resources from one hardware/software generation to the next'.[6] The second means of overcoming such technological obsolescence is *emulation*, which focuses on 'developing techniques for imitating obsolete systems on future generations of computers'.[7]

It is one of the goals of the TIMBUS project to take digital preservation into the business domain, whereby existing digital preservation knowledge[8] is applied to business processes. These efforts serve the goal of being able to recover, for instance, a production process at any given time in the future without the loss of either time or information. The phases that are necessary to preserve and later on recover information represented in business processes and digital objects, respectively, can be summarized into three gross categories: expediency, execution and exhumation. In the course of the *expediency* or preservation planning phase, the feasibility of digital preservation for a concrete entity is evaluated. A risk management approach is taken, whereby the critical business processes, but also the boundaries to the envisioned preservation solution, set, inter alia, by intellectual property rights or data protection laws, are identified. Furthermore, the significant characteristics of the identified business processes that need to be maintained over time are defined. The *execution* phase refers to the actual implementation of the previously developed preservation plan. It also encompasses the setting up and optimizing of IT contracts needed to balance the interest of the stakeholders involved in the preservation efforts. Lastly, the *exhumation* or redeployment phase comprises all steps necessary to rerun business processes in a new environment in the future. The verification of the correct behaviour of the redeployed processes forms an integral part thereof.

---

[6] Jones and Beagrie 2008: 26.

[7] *Ibid.* 25.

[8] For an overview of current research projects dealing with digital preservation issues, see Strodl, Petrov and Rauber 2011.

2. Legal aspects of digital preservation

European Directives as well as national laws and regulations have a large impact on the possibilities of how to use a digital preservation system. Nevertheless, a holistic legal understanding of digital long-term preservation is missing.[1] Some regulations that affect the possibilities of digital preservation systems are obvious. In particular, the laws of data protection and intellectual property rights (IPRs) have to be considered; and, of course, one will need to consider IT contracting issues, such as service level agreements or IPRs licensing in general. But besides these obvious legal issues, a holistic digital preservation system will be affected by many different laws and regulations. Even if the number of European regulations and national laws is finite, it is quite impossible to consider every single law of 28 Member States and analyse their impact on a digital preservation system for business processes, especially if one analyses only abstract processes without a concrete reference to a company, or at least a concrete branch. It is rather necessary to take a closer look at legal problems, while creating a concrete digital preservation system for a concrete company. The aim of this legal analysis of digital preservation systems for business processes is not to give answers to unasked and unknown questions, but to create the awareness that one will need to take a closer look at many legal problems which arise with the creation of a holistic digital preservation system for business processes. Therefore, we shall begin our discussion with some legal aspects arising in different fields of law, which may not be as obvious as data protection or IT contracting. In general, one can distinguish three different main fields of law: private law, public law and criminal law; in each field one will find regulations with an impact on digital preservation systems.

[1] See Strodl, Petrov and Rauber 2011: 23.