JABATAN PERLINDUNGAN DATA PERIBADI
Kementerian Komunikasi dan Multimedia Malaysia

PEMATUHAN AKTA PERLINDUNGAN DATA PERIBADI (AKTA 709)

(STANDARD PERLINDUNGAN DATA PERIBADI)

Apa itu STANDARD?

AKTA 709

SUBSIDIARI P.U.(A) 335

- Suatu **kehendak minimum** yang dikeluarkan oleh Pesuruhjaya;
- Bagi **kegunaan biasa yang berulang-ulang;**
- **Kaedah-kaedah, garis panduan** bagi aktiviti atau keputusan aktiviti itu

PUNCA KUASA:
AKTA 709

SEKSYEN 143, AKTA 709

SUBSIDIARI
P.U.(A) 335

- **Para. 6 – Standard Keselamatan**
- **Para. 7 – Standard Penyimpanan**
- **Para. 8 – Standard Integriti Data**

14 November 2013
14 November 2013
P.U. (A) 335

WARTA KERAJAAN PERSEKUTUAN

FEDERAL GOVERNMENT GAZETTE

PERATURAN-PERATURAN PERLINDUNGAN DATA PERIBADI 2013

PERSONAL DATA PROTECTION REGULATIONS 2013

Kronologi Pembangunan Standard

2014

- 8 perbincangan tidak rasmi
- 5 perbincangan rasmi dengan agensi (Jabatan Standard Malaysia, CyberSecurity, SKMM serta wakil-wakil industri)

2015

- Mesyuarat rasmi:15 & 23 Jun 2015, 27 Julai 2015
- Konsultasi awam:1 hingga 27 Julai 2015
- Pembentangan kepada wakil industri: 1 Ogos 2015
- Pendaftaran Standard: Tahun 2015 (jangkaan)

Information Security Management System (ISMS)

PDPA Mapping

Standard Perlindungan Data Peribadi 2015

Sumber Rujukan

MALAYSIA:
ISMS Controls;
CyberSecurity Mapping

KESATUAN EROPAH:
EU Directive 95/46/EC

UNITED KINGDOM:
Data Protection Act 1998

IRELAND:
Guide For Data Controllers, Data Protection Act 1998 and 2003

JERMAN:
Germany Federal Privacy Act

HONG KONG:
Personal Data (Privacy) Ordinance (Cap.486)

SINGAPORE:
Personal Data Protection Act 2012

BAHAMAS:
A Guide For Data Controllers, Data Protection (Privacy of Personal Information) Act 2003

Kepentingan Standard Perlindungan Data Peribadi

- Perdagangan antarabangsa
- Pelaburan asing
- Aktiviti e-Commerce

- Melindungi kepentingan negara, perniagaan, subjek data

- Penerapan budaya perlindungan data peribadi dalam tadbir urus organisasi

Kandungan Standard Pelindungan Data Peribadi

Keselamatan

Penyimpanan

Integriti Data

PEMATUHAN AKTA 709

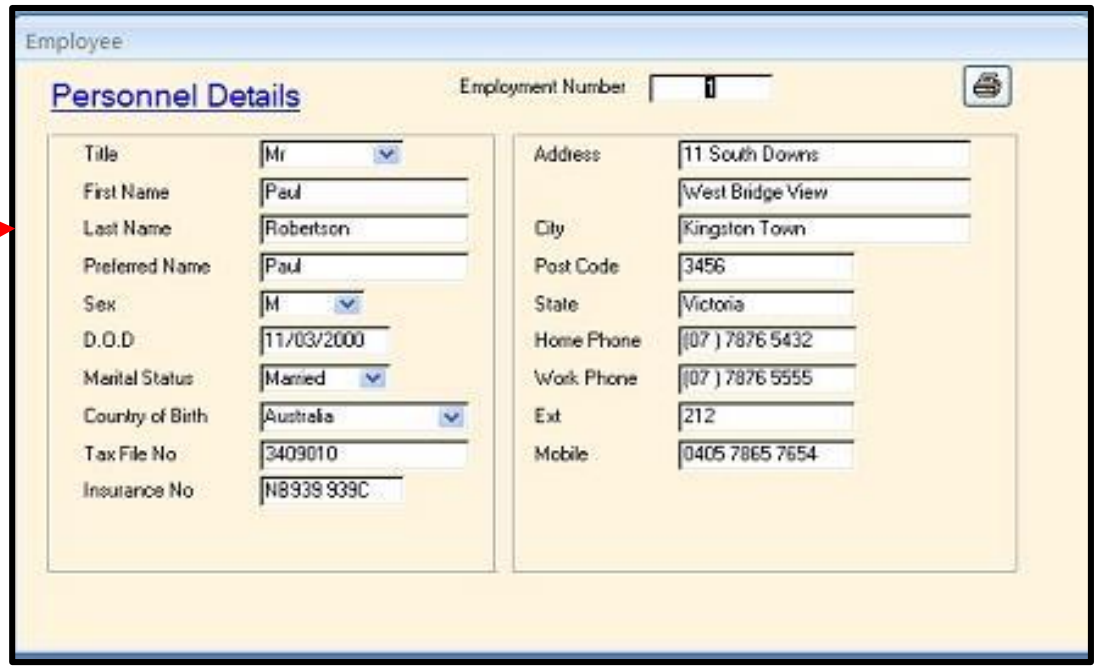
Standard Keselamatan

KESELAMATAN

- Elektronik
- Konvensional

Pendaftaran:

- **Sistem Pendaftaran Pengguna Data**



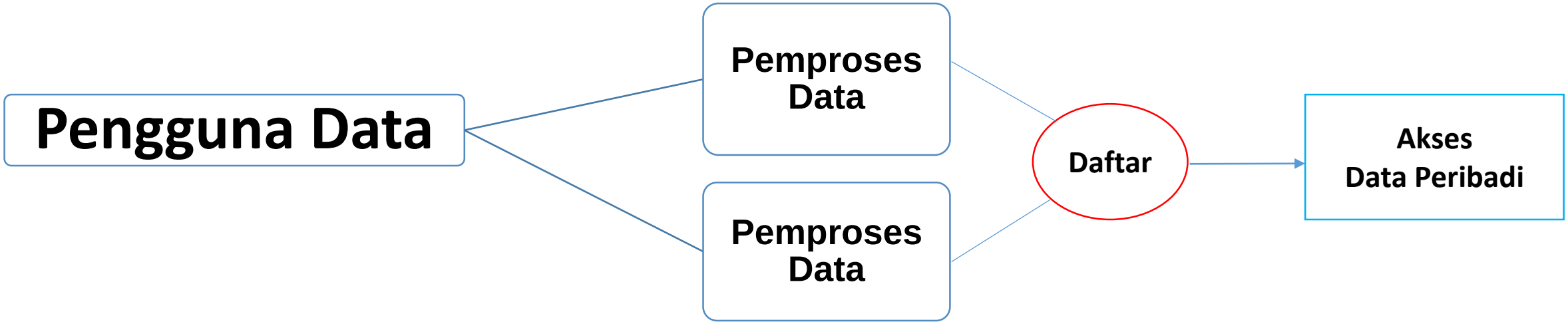
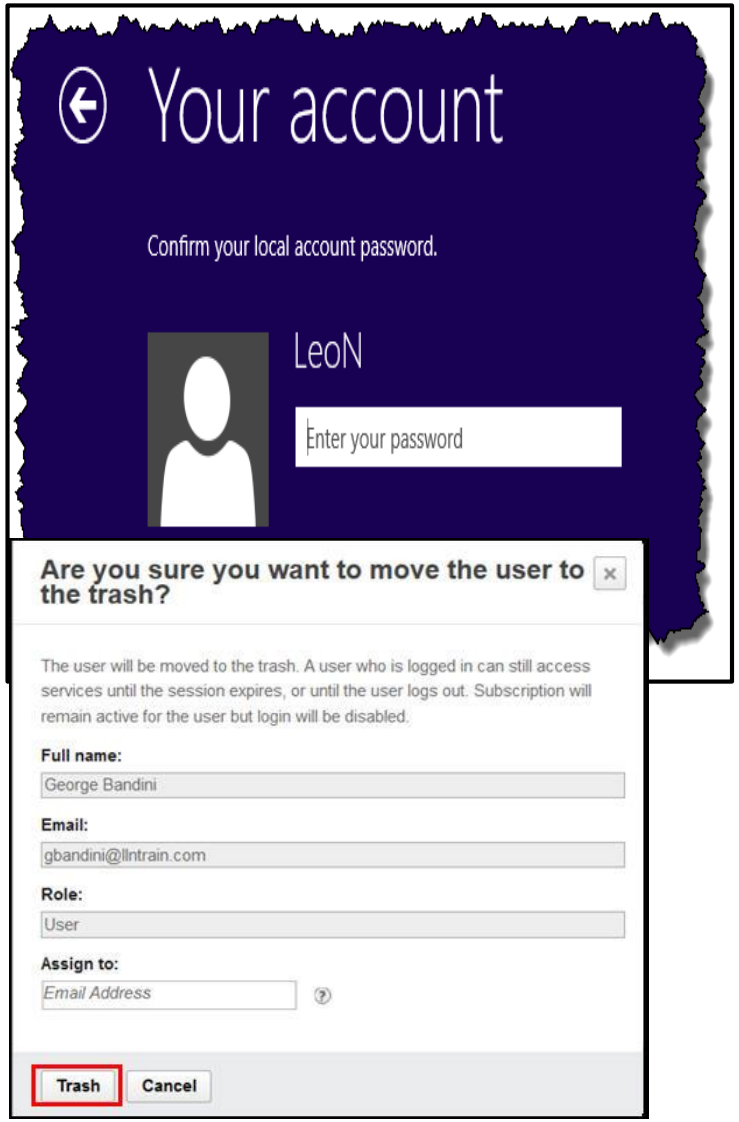


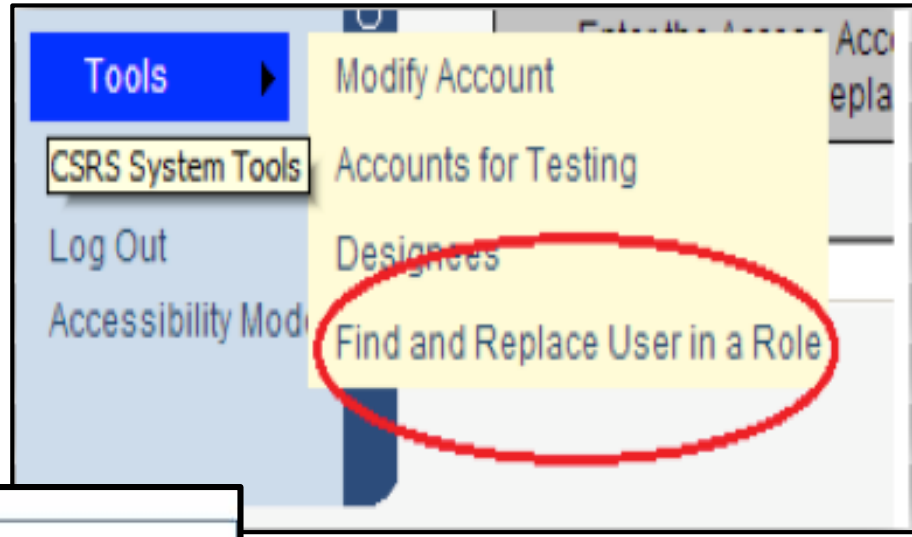
Diagram 1

Akses Sistem Data Peribadi:

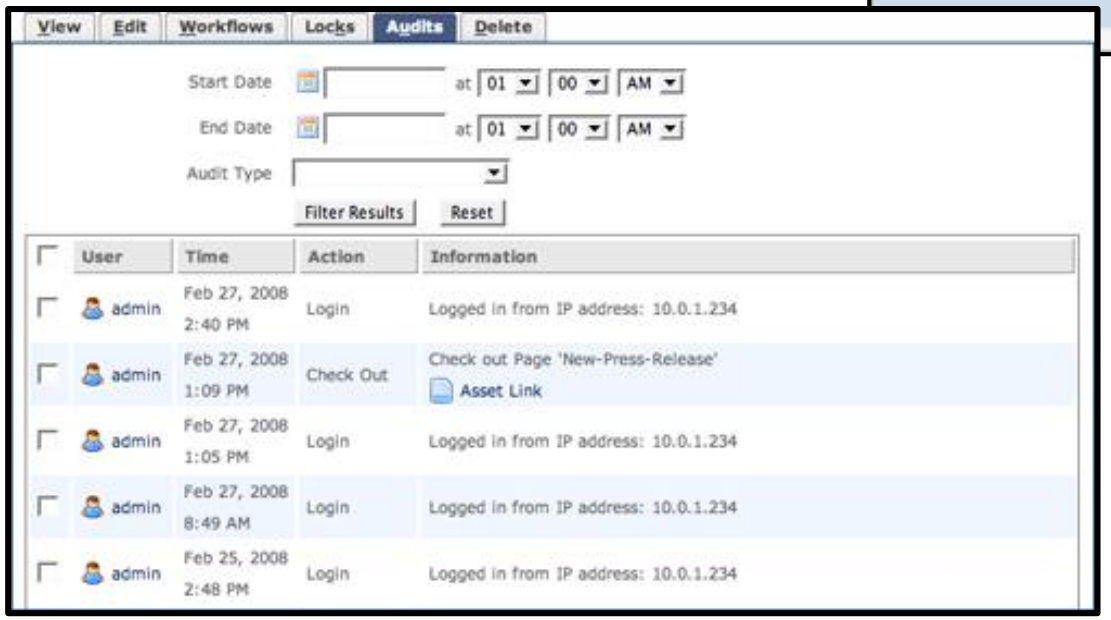
Hak akses



Takat kuasa

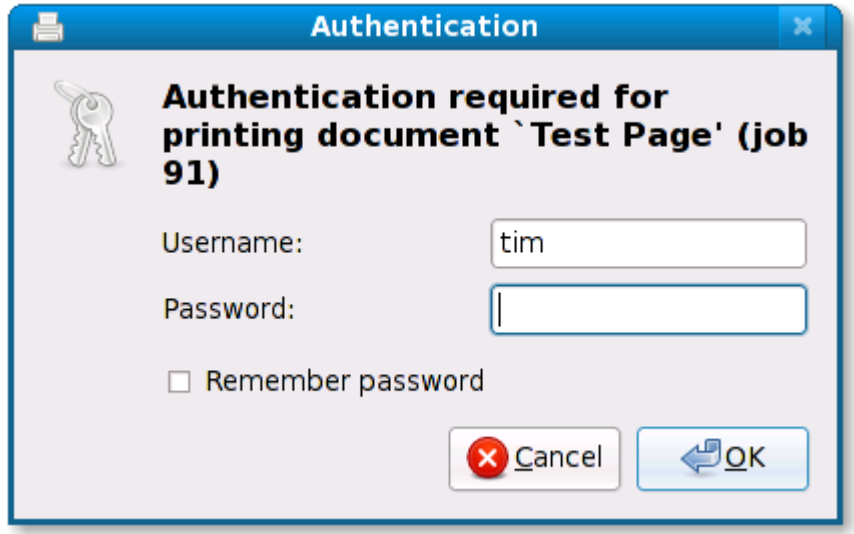


Log akses



ID Pengguna dan Kata Laluan

- Kakitangan yang menguruskan data peribadi sahaja diberikan ID Pengguna
- ID pengguna perlu dibatalkan serta merta jika kakitangan tidak menguruskan data peribadi
- Tidak berkongsi atau mendedahkan kata laluan
- *User authentication* dilaksanakan sebelum akses ke sistem data peribadi



Insiden Keselamatan Kata Laluan

NEWS

Hyatt resets Gold Passport passwords after security incident

Credit: Lane Pearman

Dropbox Spam Attack Tied to Stolen Employee Password

By NICOLE PERLROTH AUGUST 1, 2012 1:23 PM Comment

Email

Share

Tweet

Save

More

A spam attack on users of Dropbox, the cloud-storage service, has been linked to a password that was stolen in a breach on another Web site.

That is the conclusion of a two-week-long investigation by Dropbox into reports that a security breach may have caused its users to receive spam messages. The problems first surfaced July 16 after Dropbox users complained that spam messages had been sent to e-mail addresses they reserved exclusively for their Dropbox accounts. The fraudulent e-mails appeared to be from gambling sites.

In a blog post, Dropbox said that user names and passwords exposed in breaches on another Web site were tested on Dropbox accounts. And in one case, hackers used a stolen password to log into a Dropbox employee's account that contained a document with users' e-mail addresses. Spammers used those e-mail addresses to send spam.

contoh-contoh insiden kebocoran maklumat melalui kecurian komputer riba & *unauthorised access*

Dumb PIN-reset Android malware found in the wild

Cyber-crime empties pockets of UK businesses about £2.8bn per year

Danielle Walker, Senior Reporter
Follow @daniellewlkr

January 27, 2014

Theft of unencrypted laptops behind Coca-Cola breach impacting 74,000

Due to a theft of unencrypted laptops at Coca-Cola, around 74,000 current and former employees at the company may be at risk of identity theft or fraud.

Social Security numbers, driver's license numbers and other data was exposed.

Sensitive information that was on the laptops included names and Social Security numbers of around 18,000 individuals, while an additional 56,000 people had personal information, such as driver's license numbers, exposed in the incident.

Other data, like addresses, financial compensation and ethnicity of victims, was also compromised, according to a Friday article in *The Wall Street Journal*, which broke the story.

China Unveils Overhaul of Bloated State Sector

Shire May Sweeten Baxalta Bid

GM, Ford Bet on SUVs in Europe

BUSINESS

Coca-Cola: Stolen Laptops Had Personal Information of 74,000

Stolen Laptop Information Includes Social Security, Driver's License Numbers

By MIKE ESTERL
Updated Jan. 24, 2014 9:37 p.m. ET

Coca-Cola Co. said on Friday that personal information on as many as 74,000 employees, contractors and suppliers were on laptops that it said were temporarily stolen from its Atlanta headquarters.

Lokasi Penyimpanan Data Peribadi:

- Selamat
- Tidak terdedah / bertanda dengan jelas

Keselamatan fizikal:

- Pengesahan identiti sebelum memasuki kawasan pemprosesan data peribadi
- Sekatan penggunaan peranti mudah alih/media
- CCTV dan Khidmat Kawalan Keselamatan 24 jam (sekiranya perlu)

Pemindahan Data Peribadi:

- Pemindahan data peranti media mudah alih adalah tidak dibenarkan melainkan dengan kebenaran bertulis oleh pegawai yang diberi kuasa

contoh-contoh insiden kebocoran maklumat melalui peranti media / storan mudah alih

Mail Online

Barclays security scandal: Police find stolen USB stick holding personal data of 13,000 customers, including National Insurance numbers and passport details

- Police found the memory stick by chance during arrest in Brighton, Sussex
- Found on it were names, dates of birth and addresses of 13,000 customers
- Barclays says there is no evidence the files had been used by fraudsters
- Furious customers branded £250 offered in compensation an 'insult'

By RICHARD MARSDEN and JAMES SALMON FOR DAILY MAIL

PUBLISHED: 21:00 GMT, 24 July 2015 | UPDATED: 02:11 GMT, 25 July 2015

Barclays to compensate customers for losing USB stick containing personal data

Wronged punters could get £250 each

By Dave Neal

Tue Jul 14 2015, 12:16

BARCLAYS BANK will pay £250 to customers who were put at risk when a USB stick ended up in the wrong hands.

Barclays, which presumably moves sensitive customer data around on USB sticks, has been stung to the tune of £500,000 in compensation payments, according to reports.

This sort of thing might take the shine off the imminent backing of Apple Pay which, in case you missed it, has hit the UK.

UK insurer loses storage device with sensitive customer data

By Juha Saarinen
Sep 14 2015
6:31AM

Names, addresses, bank account details leaked.

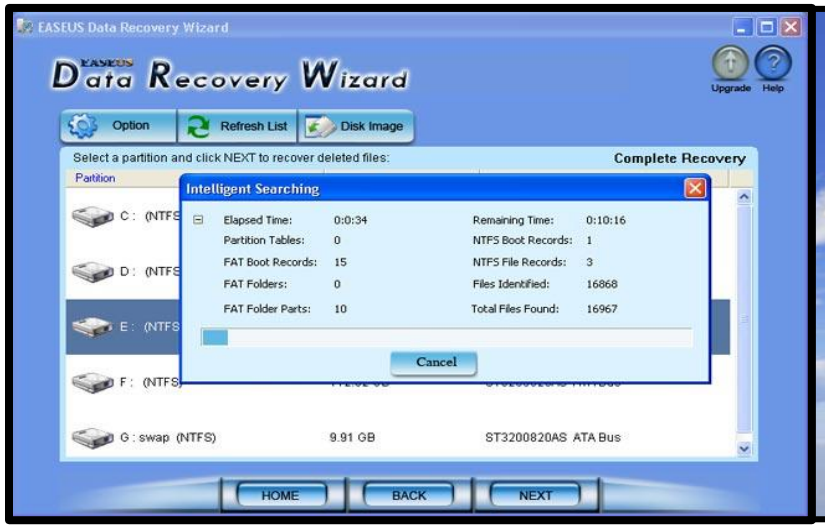
British insurer Royal Sun Alliance has owned up to losing a storage device that contained personal information on premier customers of Lloyds Bank.

The portable storage device – RSA Insurance did not provide detail on the type of device – went missing from one of the insurer's data centres on July 30. It has since been reported to police as stolen.

Back Up / Recovery Sistem

- Sistem “Back up/Recovery” serta perisian anti-virus perlu dikemaskini bagi melindungi data peribadi

- Sistem “Back up/Recovery” perlu disimpan di lokasi yang berbeza daripada lokasi utama serta selamat dari sebarang ancaman/bencana



contoh-contoh insiden pencerobohan pangkalan data (database)

Two million customers affected

The European mobile giant said personal details of more than two million of its German customer base have been stolen by a hacker.

By Zack Whittaker for Between the Lines | September 12, 2013 -- 13:58 GMT (21:58 GMT-08:00) | Topic: Security

RELATED STORIES

Security
Intel launches automotive security board to tackle connected car security risks

Security
Meet the worst 100 passwords fro the Ashley Madison hack

HNGN

MONDAY, SEPTEMBER 14, 2015
NEWS FOR A MOBILE GENE

STARS & THEIR PETS EXCLUSIVE: Dean Cain And His Dogs Happy A...

HNGN's Rescue Pet Of The Week Is NYC Cat Emmaline! 'Meet You...

Fire At Samsung Datacenter Cause Outage On Easter (TWEETS)

A fire broke out at a Samsung data center in South Korea Sunda service outages for its global website and smart TV apps.

By Sam Lehman | Apr 21, 2014 10:41 AM EDT

TECHNEWSWORLD

DATA MANAGEMENT

Data Center Fire Fries Samsung's Un-Backed-Up Servers

Stuff happens -- but that's why the IT departments of major corporations are supposed to back up their stuff. Samsung SDS apparently failed in the remote backup department, and when a fire swept through its data center, a massive service outage was the result. "There really is no excuse for this to occur," said Tirias Research analyst Jim McGregor.

Data yang diproses secara konvensional juga perlu dilindungi dengan sewajarnya

Konvensional-1

Pendaftaran:

- Mewujudkan sebuah buku pendaftaran fizikal bagi mendaftarkan semua kakitangan yang terlibat dalam pemprosesan data peribadi

Akses:

- Notis pembatalan kebenaran akses dikeluarkan dengan segera

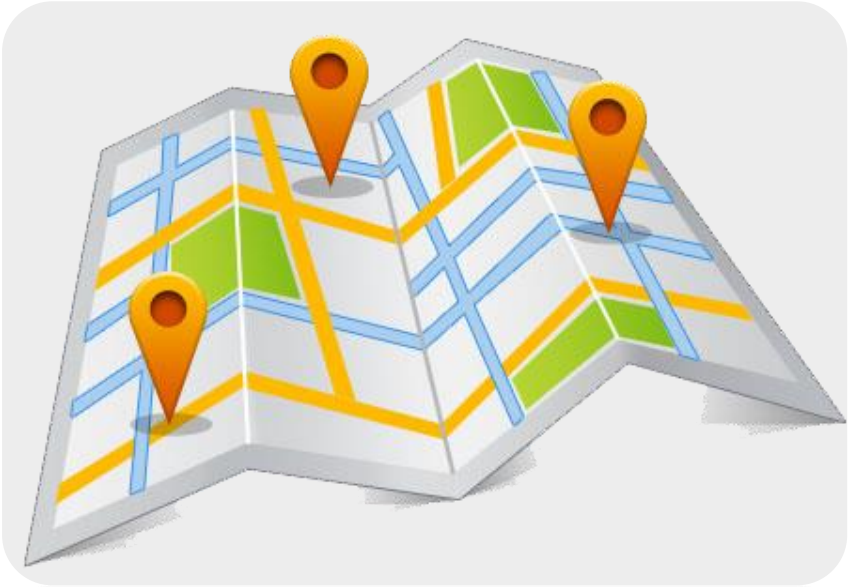
Konvensional-2

Takat Kuasa:

- Data peribadi hanya boleh diakses oleh kakitangan yang ditetapkan sahaja

Lokasi:

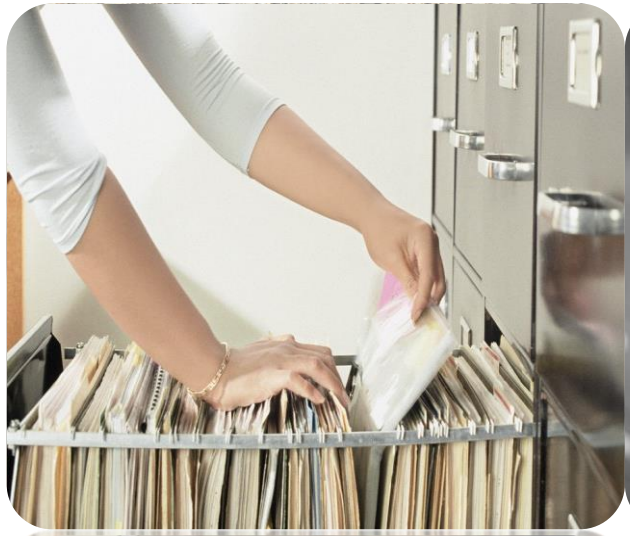
- Selamat
- Tidak terdedah/ bertanda



Konvensional-3

Keselamatan fizikal:

- Data peribadi hendaklah disimpan dalam fail
- Fail yang mengandungi data peribadi hendaklah disimpan di cabinet berkunci
- Semua kunci yang berkaitan perlu disimpan di tempat selamat
- Hanya seorang sahaja diberi kebenaran memegang kunci (bergantung kepada keperluan organisasi)



contoh insiden kehilangan rekod

Konvensional-4

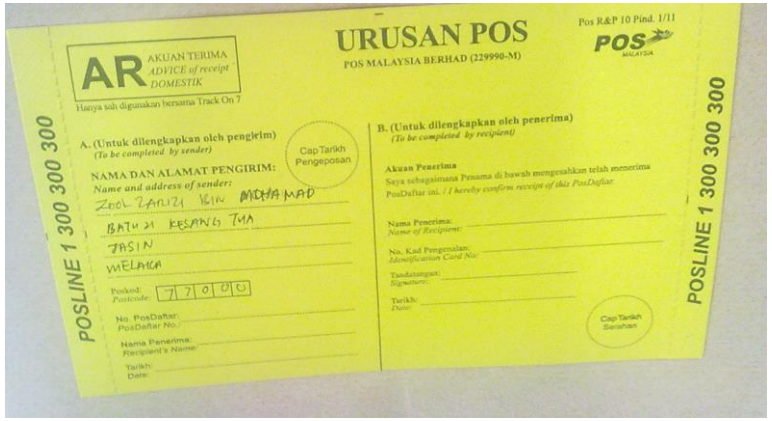
Pemusnahan Data Peribadi:

- Musnahkan data peribadi dengan kaedah yang bersesuaian.
- Merekod pemusnahan data peribadi

Konvensional-5

Pemindahan Data Peribadi:

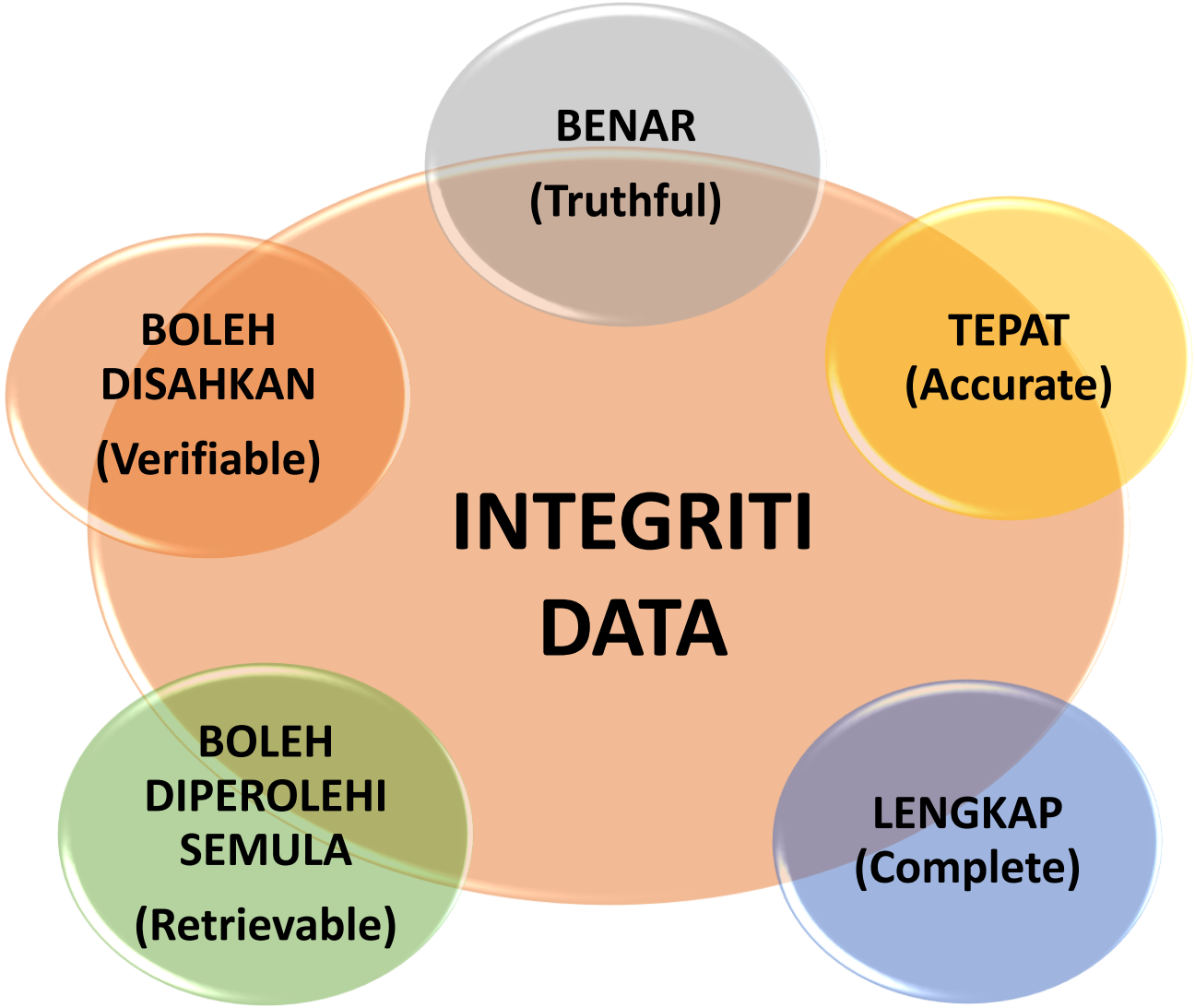
- Pos berdaftar
- Serahan tangan



Standard Integriti Data

Standard Integriti Data

- Sediakan borang kemaskini data peribadi (online/off line)
- Kemaskini data peribadi dengan segera selepas dapat notis pembetulan
- Pastikan dokumen sokongan adalah tepat dan sahih sebelum mengemaskini data peribadi



Impak Pengabaian Integriti Data

Two Indian manufacturers cited by FDA for data integrity issues

By Zachary Brennan+

04-Feb-2015

Last updated on 04-Feb-2015 at 09:25 GMT

Related tags: Micro Labs, Apotex, Warning letter, US FDA

Bangalore, India-based Apotex and Verna, India-based Micro Labs both received warning letters last month from the US FDA detailing data integrity questions linked to their quality systems.

The US FDA said the examples outlined in the letter for Apotex "*are of serious CGMP violations demonstrating that your quality system does not adequately ensure the accuracy and integrity of the data generated at your facility to ensure the safety, effectiveness, and quality of the drug products you manufacture. We found that your quality system failed to ensure the adequate investigation and resolution of quality failures.*"

The history of the company's working with the FDA to resolve cGMP violations is extensive. In April, the agency banned the facility from importing its products to the US, while back in March 2012, Apotex sued the agency over a similar import alert.

Indian manufacturers struggling to stay on top of data integrity issues, EY survey finds

By Zachary Brennan+

08-Jun-2015

Related tags: Data integrity, Indian pharma, Import alerts, Warning letters, GMP

Standard Penyimpanan

Standard Penyimpanan

Tentukan semua perundangan berkaitan penyimpanan dan pemprosesan data peribadi dipatuhi

Contoh:

- Akta Pencegahan Pengubahan Wang Haram dan Pencegahan Pembiayaan Keganasan 2001
- Akta Arkib 2003
- Akta berkaitan Insurans, Kewangan dan lain-lain

Tidak menyimpan data peribadi setelah transaksi komersil tamat **melainkan terdapat peruntukan undang-undang yang mengkehendaki** dan membenarkan penyimpanan tersebut

HALA TUJU

Penguatkuasaan

Tadbir Urus Data Peribadi

KESAN JANGKA PANJANG

CONTOH

Pematuhan Perlindungan Data Peribadi dalam e-Commerce

Newsletter

Subscribe to our newsletters now and stay up-to-date with new collections, the latest lookbooks and exclusive offers.

Introduce your email address

Sign up now

HELP
FAQS
ORDER TRACKING
DISPATCH
PAYMENT METHODS
RETURNS

BRANDS
MANGO
MANGO MAN
MANGO KIDS
VIOLETA BY MANGO

SHOPPING
GIFT VOUCHER
MANGO VIP CARD
SIZE CONVERSION CHART
SEARCH STORES
GARMENT LOCATOR
APPS

COMPANY
ABOUT MANGO
PRESS OFFICE
FRANCHISES
WORK WITH US
ENGINEERING AND CONSTRUCTION

 Privacy Policy Terms & Conditions

PRIVACY POLICY

DATA TREATMENT

Latest version: 3 November 2014.

INTRODUCTION

Access and use of the **www.mango.com** website (hereinafter, "Website" or "Mango.com ") confers user status upon visitors to the website and implies full acceptance without reservation of the conditions of use applicable at any moment on the part of the user.

In accordance with the provisions of Organic Law 15/1999, on the Protection of Personal Data (LOPD) and its implementing legislation, Mango, as manager of the website, pursuant to the provision contained in art. 5 and 6 of the LOPD, informs all website users who provide or will provide their personal details that the same will be included on a computerised file that is duly registered at the Spanish Data Protection Agency.

WHO IS THE OWNER OF THE DATA TREATMENT?

Details of the **www.mango.com** website owner and manager:

PUNTO FA, S.L. (hereinafter, "Mango")

Calle Mercaders 9-11
Pol. Ind. Riera de Caldes
C.P. 08184 Palau-solità i Plegamans
Barcelona (Spain)

E-mail: customer.service@mango.com
Tel. +34 93 860 24 24
Fax (+34) 938 602 207

Registered at the Mercantile Register of Barcelona under Volume 11195, Folio 156, Sheet 167948 and with Corporate Tax ID no. ES-B59088948.

Foundation
Burberry Group Plc
Careers
Site Map
Legal & Cookies
Terms & Conditions
Privacy Policy
Cookie Policy
Credits
Corporate Responsibility
Privacy Policy

Burberry Limited [GB] https://my.burberry.com/legal-cookies/privacy-policy/

In addition, for quality control and training purposes, we may monitor or record your communications with us.

We will at all times seek to comply with the requirements of UK Data Protection Act, 1998 (the **"Act"**) and any applicable laws and regulations to ensure that the personal information you give us is kept appropriately secure and processed fairly and lawfully. Your data will be held and managed by Burberry Limited of Horseferry House, Horseferry Road, London SW1P 2AW who will act as Data Controller for the purposes of the Act. Please contact the Burberry Legal Department on +44 (0) 20 3367 3000 if you have any queries in relation to your data.

RETENTION AND DELETION OF PERSONAL INFORMATION

We shall only keep your information as long as you remain an active customer and for 3 years afterwards or as otherwise required by law.

If you wish to request the deletion of your personal details, or wish to change your preferences at any time please contact our Customer Service Team.

MoRewards

Privileges
Terms and Conditions
Frequently Asked Questions

New Customer

Your Account

Privacy & Policy

MPH Bookstores Sdn Bhd is committed to ensuring that your privacy is protected. This privacy policy is formulated in accordance with the Personal Data Protection Act 2010, which describes how your information is collected and used and your choices with respect to your Personal Data. This policy explains how we use the information we collect about you and the procedures that we have in place to safeguard your privacy whilst you use the website.

MPH Bookstores Sdn Bhd may disclose to third party service providers within and outside of Malaysia certain aggregate information contained in your registration applications but MPH Bookstores Sdn Bhd will not disclose to any individuals your name, address, email address or telephone number without your prior consent except to the extent necessary or appropriate to comply with applicable laws or in legal proceedings.