

Loyalty Partner Group: Data Protection – Training

Munich, 2021

Dr. Robert Selk, LL.M.

Data Protection Officer Loyalty Partner Group (External)

- Introduction Dr. Robert Selk
 - (External) Data Protection Officer (DPO) of the LP Group
 - Appointed since 2009 for
 - Loyalty Partner GmbH
 - PAYBACK GmbH
 - PAYBACK Rabattverein e.V
 - Loyalty Partner Solution GmbH
 - As well as for other clients, like
 - VOLVO, LEGO, Bavaria Filmgruppe, HILTON, etc.
 - As well
 - Lawyer and Certified Lawyer for IT-Law, Partner of a Law firm
 - Co-Founder of a software company for CRM-Software
 - Instructor, Speaker and Author for Data Protection topics

 [Informieren](#) [Online Punkten](#) [Filialen & Pros](#)

[Informieren](#) » Datenschutz

DATENSCHUTZ BEI PAYBACK



Liebe Kundin, lieber Kunde,

Millionen Menschen in Deutschland genießen die Vorteile, die ihnen das größte Vergnügen mit ihren Daten. Denn bei PAYBACK hat Datenschutz eine hohe Priorität.

Dr. Robert Selk
Datenschutzbeauftragter
PAYBACK GmbH

- Examples





Datenschutzverstöße

H&M soll 35 Millionen Euro Bußgeld zahlen

Jahrelang hat die Modekette H&M Angestellte in einem Servicecenter überwacht und Angaben zu Krankheitsdiagnosen in Mitarbeiterprofilen gespeichert. Hamburgs Datenschutzler verhängt ein Rekordbußgeld.

01.10.2020, 11.41 Uhr



H&M hat Angestellte in einem Servicecenter überwacht. Foto: Mike Segar / REUTERS

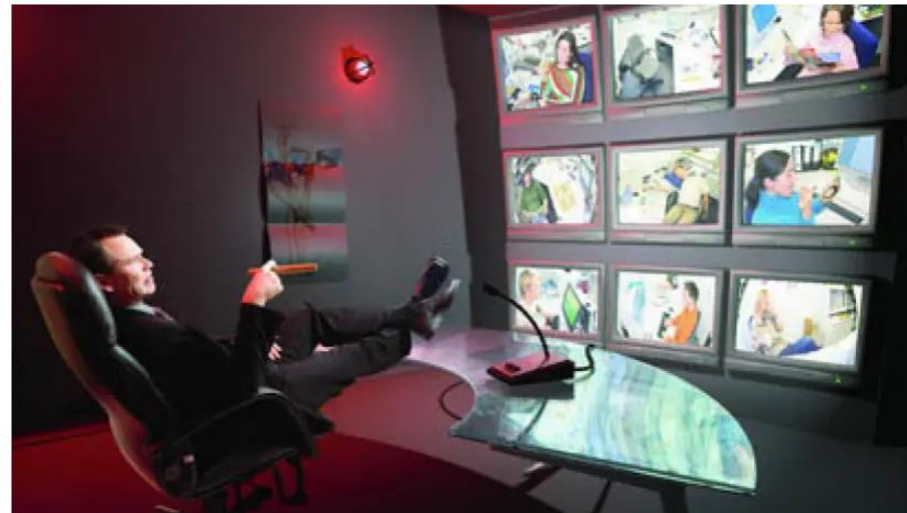
Der hamburgische Datenschutzbeauftragte Johannes Caspar verhängt ein Rekordbußgeld in Höhe von 35.258.707,95 Euro gegen das

Millionen-Bußgeld wegen Videoüberwachung gegen notebooksbilliger.de

Der Elektronikhändler notebooksbilliger.de soll 10,4 Millionen Euro Bußgeld zahlen, weil er laut Landesdatenschutzbehörde Mitarbeiter mit Kameras überwacht hat.

Lesezeit: 2 Min.  In Pocket speichern

   607



(Bild: Heise)

- What is „Data Protection “?

A **What is Data Protection?**

B What's allowed?

C Data Protection Organization in the LP Group

What is data protection?

- What is „Data Protection“?
 - Not: Protection of Data (that would be the data security!)
 - But: Protection of people from „datafication“ („verdaten“) by third parties (government or companies)
 - Better: Protection against data
 - Not: Protection of the data

What is data protection?

- Follow up question: So who protects the data?
 - Not „Data Protection“
 - See above
 - Legal topic (“not allowed to”)
 - But: The so called „Data Security“
 - Also: IT-Security, Information-Security, etc.
 - This is the „real“ protection of the data, by
 - Encryption, Backups
 - Role- and authorization concept
 - Locked doors, video surveillance
 - Etc.
 - Technical topic (“not able to”)

What is data protection?



Rust protection = Doesn't protect the rust, but protects from rust

What is data protection?

- How to achieve?
 - Laws must be established, which define how people may be datafied by businesses, government, etc.
 - „Data Protection laws“
 - Meaning in the EU:
 - GDPR as an European law act – it is „the“ EU-Super-Data protection act



- Only a very few national „Mini-Data Protection Laws“ are allowed besides the GDPR
 - Germany: BDSG, TMG, etc.
 - But these are lower-ranking, GDPR is at the very top of all data protection laws

What is data protection?

- When „data protection“ is necessary?
 - By referencing data to a specific person
 - So called „personal data “
 - → Only such data is covered by Data Protection
- This is an important question
 - Because only then Data Protection laws applies!
- Definition by Law:

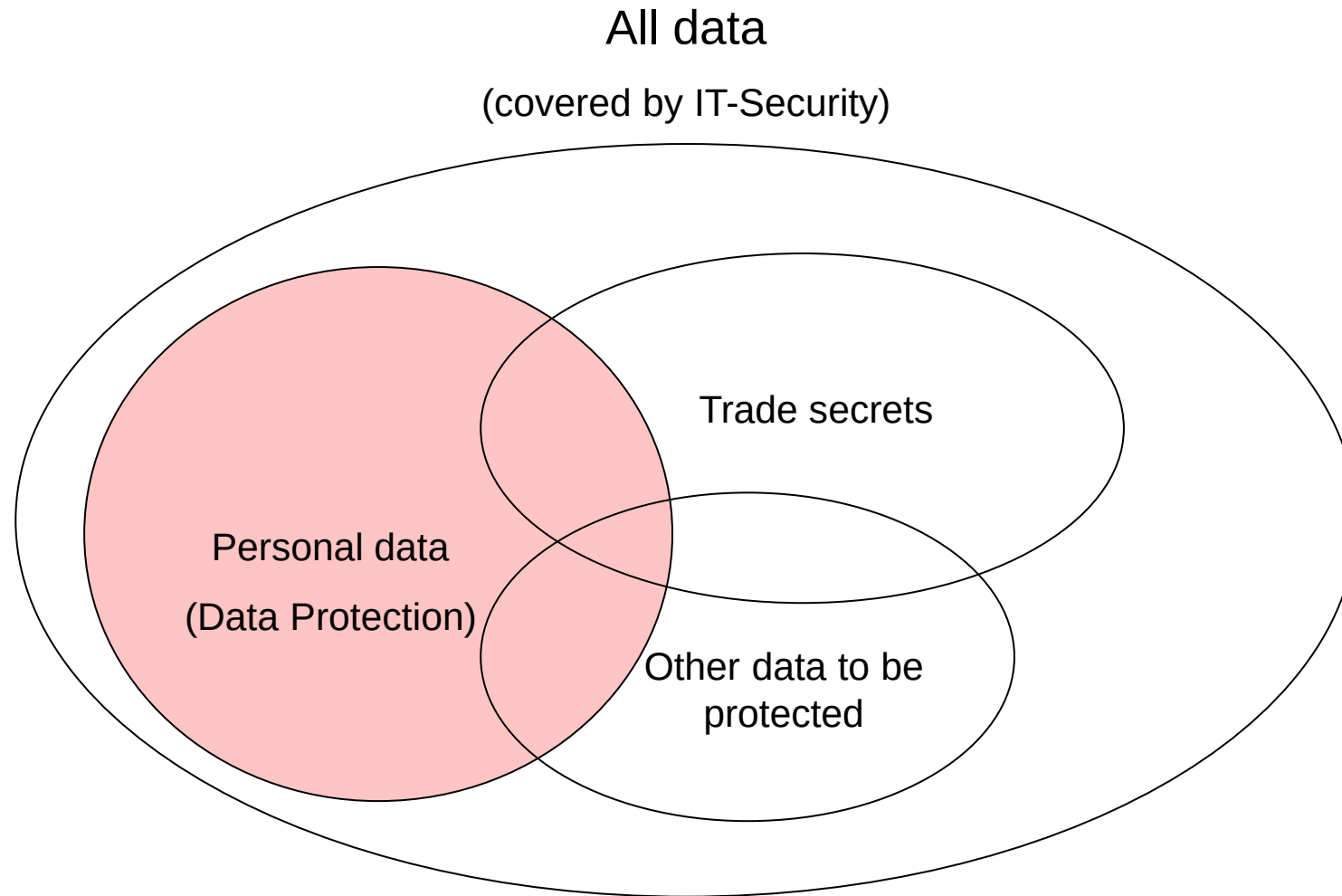
“‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’);

an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”

What is data protection?

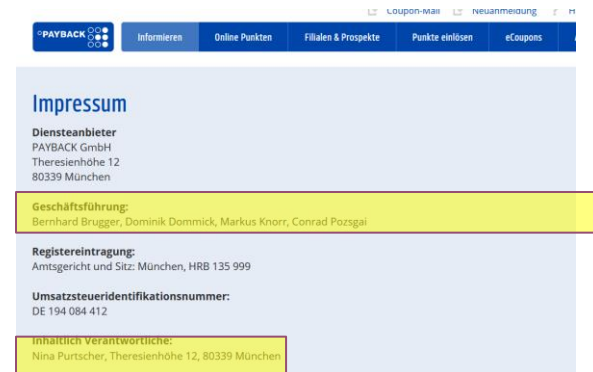
- Identified individual
 - The identity of the data subject derives directly from the data
 - Examples
 - Name: Robert Selk
 - Email address: robert.selk@xy.de
 - EC card with name
- Identifiable individual: That's enough!
 - Identity can be determined with additional information
 - Depends on what additional information is attainable
 - Important: Knowledge within a company is attributed to the whole company!
 - Example:
 - PAYBACK number → can be attributed to someone within PAYBACK
 - Mail address → you can go there and have a look
 - IP address → identity attainable by criminal proceedings
 - TRX data, usage behavior → are attributed to a member

What is data protection?



What is data protection?

- Question
 - Is data of a website imprint („Impressum“) within the scope of the data protection laws?

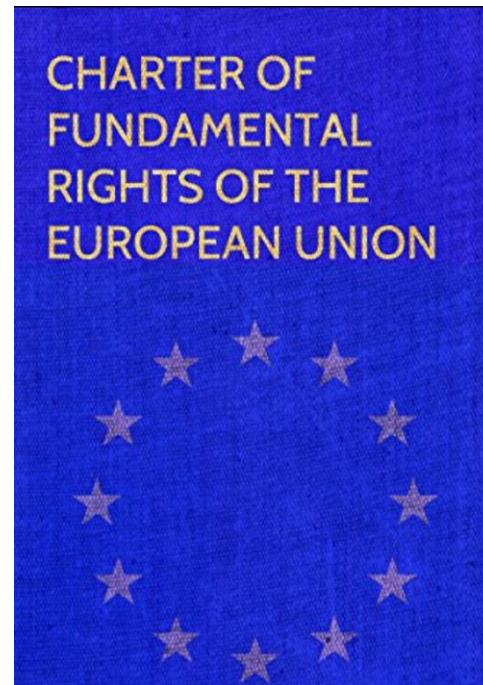


- Is this data related to a person – yes or no?
 - Answer: Of course yes, related to the named persons
 - -> “personal data”
 - According to GDPR: No matter whether data is public or not – as long there is an identifiable person, it is “personal data”
- Answer: Yes, data protection laws do apply for personal data in an imprint

- A What is Data Protection?
- B What's allowed?**
- C Data Protection Organization in the LP Group

What is allowed?

- In the whole EU
 - Data protection = Fundamental right/ Human right !



What is allowed?

TITLE II FREEDOMS

Article 6

Right to liberty and security

Everyone has the right to liberty and security of person.

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Article 9

Right to marry and right to found a family

The right to marry and the right to found a family shall be guaranteed in accordance with the national laws governing the exercise of these rights.

Article 10

Freedom of thought, conscience and religion

1. Everyone has the right to freedom of thought, conscience and religion. This right includes freedom to change religion or belief and freedom, either alone or in community with others and in public or in private, to manifest religion or belief, in worship, teaching, practice and observance.
2. The right to conscientious objection is recognised, in accordance with the national laws governing the exercise of this right.

What is allowed?

- Collect and process personal data is - from a legal perspective - a „fundamental right violation“



=



What is allowed?

- Two general rules within the EU
 1. Every processing of personal data is prohibited (“Prohibition principle”)
 - Unless it is exceptionally permitted by
 - consent of the data subject or
 - statutory permission in the laws
 - E.g.: personal data which is (really) necessary to fulfill a contract
 2. If it is allowed: Comply with various additional legal obligations, e.g.
 - Information of the data subject, about how exactly he or she is being „datafied“
 - „Data Protection Information“, „Privacy Policy“, etc.
 - Accountability
 - Formal requirements for consent
 - Data deletion, etc.

What is allowed?

- PAYBACK as an example: Which permission do we use?
 - For no-consent customers („Non EWE“)
 - Only statutory permissions
 - E.g.: fulfillment of the PAYBACK membership contract
 - → allows the mere program operation
 - Additional data processing beyond that?
 - Only if there are other statutory permissions (there are, but only a very few)
 - For consent customers
 - Additionally: Anything which is permitted by the specific consent declaration
 - EWE 00, 06, 09
 - Newsletter-Flag, 3rd party EWE, PAY Marketing EWE

What is allowed?

- <https://www.payback.de/info/ewe09>



The screenshot shows the PAYBACK website's 'Einwilligungserklärung' (Consent Declaration) page. The page is titled 'EINWILLIGUNGSERKLÄRUNG SEIT SEPTEMBER 2009'. The left sidebar contains a navigation menu with the following items: 'Zurück', 'Anmeldung (PAYBACK Karten)', 'PAYBACK Karte', 'PAYBACK Visa Karte', 'PAYBACK American Express Karte', 'Vorhandene Karte anmelden', 'Datenschutz' (expanded), 'Fragen und Antworten', 'Hinweise zum Datenschutz' (highlighted in red), 'Philosophie Kundendaten', 'Datenschutzbeauftragter', 'Datensicherheit', 'Datenschutz auf payback.de', 'Tipps', 'Vorläufige Karte drucken', and 'Teilnahmebedingungen'. The main content area is titled 'Einwilligung in Werbung und Marktforschung' and contains the following text:

Ich erkläre mich damit einverstanden, dass das Partnerunternehmen, von dem ich meine Karte erhalten habe, und die PAYBACK GmbH mir per Post, bei der Nutzung eines PAYBACK Kundenterminals und – soweit ich diese gesondert bestellt habe – in weiteren PAYBACK Services (E-Mail, SMS/MMS, PAYBACK App) **an mich gerichtete Werbung** (z. B. Extra-Punkte-Chancen und besondere Werbeaktionen wie Sonderangebote, Rabattaktionen, Produkt- und Dienstleistungsinformationen) zusenden, die auf Basis der folgenden Daten ausgewählt wird:

- Die angegebenen Daten zu persönlichen und freiwilligen Angaben sowie ggf. meine E-Mail Adresse und ggf. der Zeitpunkt meiner An- und Abmeldung für die PAYBACK Maestro® Karte
- meine Rabattdaten (Waren/Dienstleistungen, Preis, Rabattbetrag, Ort und Zeitpunkt des Vorgangs) und
- die bei meiner Kommunikation mit PAYBACK über das PAYBACK Service Center, die Internet-Seite PAYBACK.de, die PAYBACK App oder bei Nutzung der PAYBACK Services SMS/MMS oder E-Mail oder der PAYBACK Kundenterminals anfallenden Daten.

Somit erhalte ich Sonderangebote, spezielle Punkte-Aktionen und weitere attraktive Angebote.

Des Weiteren stehen diese Daten dem Partnerunternehmen und der PAYBACK GmbH für Zwecke der **Marktforschung** zur Verfügung, damit das Angebot des PAYBACK Programms noch weiter verbessert werden kann.

Meine Daten können von der PAYBACK GmbH zudem genutzt werden, um mir **individuell zugeschnittene Angebote** zu unterbreiten, während ich beim PAYBACK Service Center anrufe, die Internet-Seite PAYBACK.de oder die PAYBACK App besuche.

Einzelheiten finde ich in **Ziffer 1 und Ziffer 2 der Hinweise zum Datenschutz**.

Mein Einverständnis kann ich jederzeit gegenüber der PAYBACK GmbH, Postfach 23 21 03, 85330 München, widerrufen.

What is allowed?

- <https://www.payback.de/info/hinweise-datenschutz>

The screenshot shows the PAYBACK website's navigation bar with links: Informieren, Online Punkten, Filialen & Prospekte, Punkte Einlösen, eCoupons, App, and a search bar. Below the navigation bar, a breadcrumb trail reads: Sie sind hier: Home > Informieren & Anmelden > Anmeldung (PAYBACK Karten) > Datenschutz > Hinweise zum Datenschutz. On the left, a sidebar menu lists: < Zurück, Anmeldung (PAYBACK Karten), PAYBACK Karte, PAYBACK Visa Karte, PAYBACK American Express Karte, Vorhandene Karte anmelden, and a dropdown for Datenschutz containing: > Fragen und Antworten, > Hinweise zum Datenschutz (highlighted in red), > Philosophie Kundendaten, and > Datenschutzbeauftragter. The main content area is titled 'HINWEISE ZUM DATENSCHUTZ' and contains the following text:

1. Ihre Daten

Wenn Sie am PAYBACK Programm teilnehmen, werden Ihr voller Name, Ihr Geburtsdatum und Ihre vollständige Anschrift benötigt (Basisdaten). Die Basisdaten und eventuelle weitere freiwillige Angaben werden durch die PAYBACK Betreibergesellschaft PAYBACK GmbH, Postfach 23 21 03, 85330 München, zur Abwicklung des PAYBACK Programms erhoben, gespeichert und genutzt. Die Basisdaten, eventuelle freiwillige Angaben und ggf. deren Änderungen übermittelt PAYBACK an das Partnerunternehmen, von dem Sie Ihre PAYBACK Karte erhalten haben. Sollten Sie Ihre PAYBACK Karte direkt von PAYBACK oder von einer Apotheke erhalten haben, erfolgt eine solche Übermittlung nicht. Wenn Sie eine PAYBACK Maestro® Karte mit Zahlungsfunktion besitzen, kann PAYBACK außerdem Änderungen Ihres Namens oder Ihrer Anschrift an die emittierende Bank übermitteln. Eine Übermittlung von persönlichen Daten an die übrigen Partnerunternehmen oder an außerhalb des Programms stehende Dritte findet – außer im Falle eines konkreten Missbrauchsverdachts – nur statt, wenn und soweit Sie gegenüber PAYBACK in diese Übermittlung gesondert eingewilligt haben (z.B. für PAYBACK Services auf der Website eines Partnerunternehmens).

Setzen Sie Ihre PAYBACK Karte bei einem Partnerunternehmen ein, so meldet dieses die Rabattdaten (Waren/Dienstleistungen, Preis, Rabattbetrag, Ort und Zeitpunkt des Vorgangs) an PAYBACK zur Gutschrift, Abrechnung gegenüber den Partnerunternehmen. Verwaltung und Auszahlung der Rabatte. Apotheken und Sparkassen melden

What is allowed?

- Conclusion:
 - For PAYBACK it is specified by
 - Either: the „PAYBACK membership contract“
 - Or: possible consent declarations
 - Comment
 - Often less, than the partners are thinking

What is allowed?

- Fines and liability
 - Monetary sanctions
 - For smaller violations: up to 10 m. € or 2 % of the worldwide corporate group annual turnover (which is higher)
 - For normal violations: up to 20 m. € or 4 % of the worldwide corporate group annual turnover (which is higher)
 - Additionally
 - Greatly expanded rights for warnings and legal action for consumer protection organisations and Data Protection authorities
 - More rights for the data subjects
 - Who is liable?
 - External liability (towards authorities, data subjects, etc.)
 - In most cases: The company (PAYBACK GmbH, etc.)
 - Exception: deliberate violations by a person -> this person is personal liable
 - Internal liability (towards the employer)
 - No Changes by GDPR
 - This person is liable which has infringed the data protection laws

- A What is Data Protection?
- B What's allowed?
- C Data Protection Organization in the LP Group**

Data Protection Organization

- Roles in Data Protection organisation in a company
 - The departments / employees
 - Here the personal data is processed, collected, used, stored, etc.
 - Here „Data protection must be done“, here it is important to know what's allowed
 - -> here is the main responsibility
 - Support by
 - Data Protection Management Team
 - Tasks: First level support, overall management, coordination, etc.
 - Legal department / GCO
 - IT Security
 - DPO – data protection officer
 - Provides advice and support the departments
 - Impartial, not bound by instruction, monitors the departments

- Current topics

Current Topics

- Current topics
 - Data Protection & Home Office
 - Please comply with the LP Home Office guidelines
 - Webex meetings
 - Please use for confidential meetings the „lock“ function
 - Handling of job applications
 - They contain often not only personal data but sensitive personal data!
 - Best is
 - Do not print
 - delete as soon as possible,
 - do not store needless or share, etc.

- Take-aways

Take-aways

1. Important to understand: Data Protection ≠ Data Security

- Data Protection = Protects the people, not the data
- Data Security = Protects the data

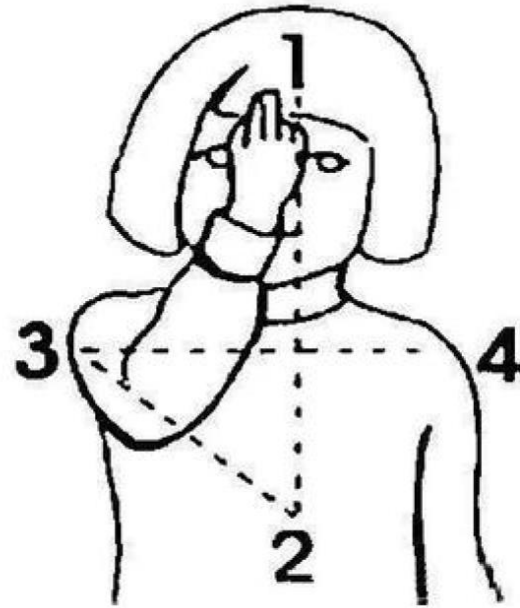
2. „Principle of prohibition“

- For each data processing a permission (consent or law) is required, otherwise it is prohibited
- Please (let) check in advance!

3. Make yourself clear: your role and your responsibility

- Please ask before something has gone wrong

4 EASY STEPS FOR GDPR COMPLIANCE



There is a movie about the GDPR

„Democracy – Im Rausch der Daten“

<https://www.youtube.com/watch?v=S825mBcGYNO> (Trailer only)



Thank you very much!

Dr. Robert Selk, LL.M.
External DPO of the LP Group

selk@dsb-consulting.com