Information à la clientèle du groupe OBT 2026



Éditorial 4

Nouvelle loi sur la transparence 5

Nouveautés dans le code des obligations 7

Abolition de l'imposition de la valeur locative – Entrée en vigueur – Planification fiscale 8

Décompte selon la méthode des taux de la dette fiscale nette 10

Cryptomonnaies et échange automatique de renseignements 12

Test de la santé informatique pour les PME 14

Guide d'autogestion pour PME 18

L'IA dans les logiciels de gestion: l'exemple d'Abacus 19

Maîtriser les cyberrisques: la sécurité commence par une prise de conscience 22

Éditorial

Au tournant de l'année 2026, de nombreuses modifications légales entreront en vigueur, qu'il s'agisse d'exigences de transparence pour les entreprises, de nouveaux délais en cas de défauts de construction ou d'ajustements du taux de TVA net. Les propriétaires qui occupent eux-mêmes leur bien immobilier devraient tenir compte de l'abolition de la valeur locative et l'échange automatique de renseignements (EAR) sera étendu aux cryptomonnaies.

En outre, le test de la santé informatique (IT-Health-Check) d'OBT SA offre aux PME un examen structuré de l'informatique, tandis qu'un guide d'autogestion aide les cadres. Si l'intelligence artificielle offre de nouvelles opportunités au secteur financier, elle entraîne également des cyberrisques.

Nous vous souhaitons une agréable lecture.



Nouvelle loi sur la transparence

Introduction d'un registre des ayants droit économiques

Avec la loi fédérale sur la transparence des personnes morales et l'identification des ayants droit économiques (LTPM), la Suisse met en œuvre les directives internationales en matière de lutte contre le blanchiment d'argent et les recommandations du Groupe d'action financière (GAFI). L'objectif des nouvelles dispositions est de rendre publiques les structures de sociétés non transparentes et d'empêcher que des personnes morales soient utilisées abusivement pour dissimuler des contextes économiques ou des avoirs illégaux.

La loi oblige les entreprises à rendre compréhensibles les rapports réels de propriété et de contrôle et crée à cet effet un registre central de transparence. La loi devrait entrer en vigueur au plus tôt au printemps 2026.

Les principales obligations, exceptions et conséquences pour les entreprises et les prestataires de services sont expliquées ci-dessous.

Saisie des ayants droit économiques

La loi sur la transparence s'applique en premier lieu aux personnes morales ayant leur siège en Suisse, dont notamment:

- les sociétés anonymes (SA) et les sociétés en commandite par actions;
- les sociétés à responsabilité limitée (Sàrl);
- les sociétés coopératives;
- les sociétés d'investissement à capital variable (SICAV) ou à capital fixe (SICAF);
- les sociétés en commandite de placements collectifs.

En outre, la loi s'applique également aux fondations et aux associations, dans la mesure où elles sont tenues de s'inscrire au registre du commerce, ainsi qu'aux personnes morales de droit étranger si elles ont une succursale en Suisse inscrite au registre du commerce; si elles ont leur administration effective en Suisse ou si elles sont propriétaires d'un immeuble situé en Suisse (ou si elles acquièrent un tel immeuble au sens de la LFAIE). La loi sur la transparence ne s'applique que partiellement aux trustees qui ont leur domicile ou leur siège en Suisse ou qui administrent des trusts en Suisse, car les trusts ne sont pas eux-mêmes des personnes morales et ne sont donc pas directement inscrits au registre de transparence. La loi n'oblige le trustee qu'à identifier et à déclarer les ayants droit économiques, tandis que les autres obligations applicables aux personnes morales (p. ex. les obligations comptables) ne s'appliquent pas.

Exclusions du champ d'application

Certaines entités juridiques sont exclues de la loi sur la transparence parce qu'il existe déjà un degré de divulgation suffisant dans leur cas. Parmi ces entités, citons:

- les sociétés cotées en bourse et filiales détenues à plus de 75 % par des entreprises cotées;
- les institutions de prévoyance professionnelle et les institutions comparables;
- les personnes morales en mains publiques dont 75 % au moins des droits de participation sont détenus par la Confédération, les cantons ou les communes.

Informations à déclarer en vertu de la loi sur la transparence

Est considérée comme ayant droit économique toute personne physique qui, en dernier ressort, exerce un contrôle sur une société, que ce soit par une participation directe ou indirecte, seule ou de concert avec des tiers, d'au moins 25 % du capital ou des droits de vote, ou d'une autre manière (p. ex. via une influence dominante). Si aucune personne de ce type ne peut être identifiée, le membre le plus haut placé de l'organe directeur (p. ex. président du conseil d'administration, président de la direction) est considéré comme l'ayant droit économique à titre subsidiaire.

Les sociétés sont tenues d'identifier leurs ayants droit économiques, de vérifier leur identité, de documenter les informations correspondantes et de les communiquer au registre de transparence.

Les informations suivantes doivent impérativement être saisies et tenues à jour en permanence:

- nom et prénom;
- date de naissance;
- nationalité;
- adresse et pays de résidence;
- nature et étendue du contrôle (p. ex. taux de participation, pourcentage de droits de vote).

La déclaration de ces informations doit être faite dans un délai d'un mois à compter de la constitution de la société et toute modification de ces informations doit être déclarée dans un délai de 30 jours à compter du moment où elles sont connues. En outre, des informations sur la personne morale elle-même doivent être communiquées – raison sociale, forme juridique, siège, numéro d'identification des entreprises (IDE) et un point de contact.

Le registre de transparence est géré par l'Office fédéral de la justice (OFJ). Il s'agit d'un registre non public, accessible uniquement aux autorités et aux organismes légalement autorisés (p. ex. les autorités de poursuite pénale, les autorités fiscales ou les autorités de surveillance des marchés financiers).

Les inscriptions, modifications et radiations sont gratuites. Les entités juridiques qui ont satisfait à leur obligation de déclaration peuvent demander au registre une confirmation de leur inscription. De même, il est possible de demander un extrait ou un extrait complet du registre.

Remarque: conformément à l'art. 13 de la loi sur la transparence, les actionnaires et les associés qui détiennent seuls ou avec des tiers le contrôle d'une société sont également tenus de fournir en temps utile à la société les informations nécessaires à l'identification et à la déclaration des ayants droit économiques. Sans cette participation, la société ne peut pas satisfaire pleinement à son obligation de déclaration.

Aménagements pour les PME

Le législateur a prévu de réduire au maximum les obligations administratives pour les petites et moyennes entreprises (PME). Pour les sociétés disposant de structures de propriété et de contrôle claires, il existe donc des procédures de déclaration simplifiées et des délais transitoires généreux pour la première saisie des ayants droit économiques.

Nouvelles obligations de diligence

La loi apporte non seulement l'obligation de tenir un registre, elle étend également les obligations de diligence prévues par la législation sur le blanchiment d'argent à certains services de conseil et de fiducie.
Sont notamment concernées les activités liées à:

- la création de sociétés;
- la gestion ou l'administration de sociétés de domicile;
- la gestion d'actifs;
- la conception de structures de participation complexes.

Importance pour la pratique

Pour les bureaux fiduciaires, les avocats et les conseillers d'entreprise, la nouvelle loi implique un surcroît sensible de travail administratif. Ils doivent en effet créer des processus internes pour assurer l'identification, la documentation et la mise à jour permanente des ayants droit économiques, et mettre en place des mécanismes de contrôle interne pour respecter les délais.

Bon à savoir

La loi sur la transparence contient des dispositions pénales en cas de non-respect des obligations de déclaration et de mise à jour. Quiconque ne communique pas les ayants droit économiques ou les communique avec retard ou de manière incomplète, encourt une amende pouvant atteindre CHF 500'000.–. Il est donc essentiel de respecter scrupuleusement les nouvelles obligations, non seulement pour des raisons de conformité, mais aussi de responsabilité.

Auteures: Nina Kurz, Samra Ibric et Carmen Marotta-von Gunten

Nouveautés dans le code des obligations

Le délai de réclamation en cas de défaut lors de l'achat d'un terrain ou d'un ouvrage immobilier est désormais de 60 jours à compter de la réception ou de la découverte du défaut. Selon le droit en vigueur jusqu'à présent, aucun délai légal explicite ne s'appliquait, mais la notification devait être faite «immédiatement». Le nouveau délai ne peut pas être raccourci (art. 219a al. 1, art. 367 al. 1bis et art. 370 al. 4 CO). Pour nos clients, cette modification de la loi est particulièrement importante, car elle a des répercussions directes sur les contrats de construction, de vente et d'entreprise. Tant les acheteurs de terrains que les entrepreneurs et les maîtres d'ouvrage devront à l'avenir respecter les nouveaux délais et les droits impératifs liés aux défauts.

La réglementation relative à la réfection des défauts de construction a également été adaptée: le droit à la réparation gratuite existait déjà, mais la nouveauté est que ce droit ne peut plus être exclu ou limité par contrat (art. 368 al. 2bis CO). Ce droit de réparation obligatoire s'applique également à l'achat d'un terrain sur lequel une construction doit encore être érigée ainsi qu'à l'acquisition d'une construction dont la construction a été achevée moins de deux ans avant la vente (art. 219a al. 2 CO).

Enfin, le délai de prescription pour les réclamations pour défauts est également uniformisé: pour les défauts affectant les ouvrages immobiliers et les terrains, le délai est désormais de cinq ans et ne peut être modifié au détriment de l'acheteur ou du client (art. 219a al. 3 et art. 371 al. 3 CO).

Bon à savoir

Nouveautés concernant les défauts de construction dans le code des obligations

- Délai de réclamation: désormais 60 jours à compter de la réception ou de la découverte du défaut (auparavant, pas de délai légal, seule la mention «sans délai» figurait)
- Droit à la réfection: le droit à une réfection gratuite ne peut désormais plus être exclu par contrat.
- Champ d'application: s'applique également aux achats de terrains avec construction à venir ou aux constructions réalisées moins de deux ans avant la vente.
- Prescription: délai uniforme de cinq ans pour les réclamations pour défauts, non modifiable en défaveur de l'acheteur ou du mandataire.

Auteures: Nina Kurz, Samra Ibric et Carmen Marotta-von Gunten

Clause de non-responsabilité: Cette information à la clientèle offre un premier aperçu des nouveautés actuelles et ne prétend pas être exhaustive. Elle ne constitue notamment pas un conseil juridique. Si vous avez des questions sur ces nouveautés ou si vous souhaitez obtenir des conseils, veuillez vous adresser à votre interlocutrice ou à votre interlocuteur au sein d'OBT SA.

Abolition de l'imposition de la valeur locative – Entrée en vigueur – Planification fiscale

Avec 57,7 % de voix pour le «oui», l'électorat s'est prononcé le 28. septembre 2025: **l'imposition de la valeur locative est abolie.**

Pour les propriétaires de logements, les conséquences varient en fonction de la situation individuelle et de la mise en œuvre cantonale. Il est recommandé de se pencher suffisamment tôt sur les changements fiscaux.

La décision en bref

- L'imposition de valeur locative est entièrement supprimée pour les **propriétés immobilières principales et secondaires utilisées par le propriétaire.**
- Les possibilités de déduire les **frais d'entretien des biens immobiliers utilisés par le propriétaire lui-même** sont supprimées, les déductions pour les **mesures d'économie d'énergie et de protection de l'environnement** ne sont plus déductibles au niveau fédéral, mais sont encore partiellement déductibles au niveau cantonal pour une durée limitée. Elles restent toutefois déductibles pour les biens immobiliers loués.
- Les **intérêts débiteurs** ne pourront à l'avenir être déduits que de manière limitée: soit sous forme de quote-part restrictive en combinaison avec des biens loués, soit dans le cadre d'une déduction spéciale pour les primo-accédants à un bien immobilier à usage personnel (pour une durée maximale de dix ans).
- Les cantons ont la possibilité d'introduire un nouvel impôt immobilier pour les résidences secondaires utilisées principalement par le propriétaire. La forme concrète de cet impôt variera d'un canton à l'autre.

Entrée en vigueur

Selon la conférence de presse du Conseil fédéral du 28. septembre 2025, le 1er janvier 2028 devrait être une date réaliste (la plus proche possible).

Durée de la période de transition

D'ici son entrée en vigueur (au plus tôt le 1er janvier 2028), la valeur locative doit continuer à être imposée comme un revenu. Parallèlement, les possibilités de déductions existantes peuvent encore être utilisées jusqu'à cette date

Fiche d'information sur la nouvelle réglementation sur la déduction des intérêts passifs

Nous vous renvoyons ici à la **Fiche d'information** «Nouvelle réglementation sur les intérêts passifs» du Département fédéral des finances DFF. Différents exemples y sont illustrés.

Période de transition – Planification fiscale

Révision de la stratégie hypothécaire

- Tant que la déduction des intérêts passifs existe encore, cela vaut la peine de détenir des hypothèques un peu plus élevées.
- Après la suppression (lorsque la déduction disparaîtra), un endettement plus faible devient plus attrayant et des amortissements sont alors rentables.

Planifier intelligemment les travaux de rénovation/d'entretien

- Mieux vaut effectuer les rénovations importantes avant l'entrée en vigueur de la réforme (d'ici le 31.12.2027) afin de profiter des avantages fiscaux
- Pensez à prendre contact suffisamment tôt avec les artisans, car cette réforme pourrait entraîner une forte demande de rénovations.

Bon à savoir

Cela vaut la peine de se pencher suffisamment tôt sur sa propre situation.
Le cas échéant, il est intéressant de procéder à des amortissements et/ou à des remboursements complets d'hypothèques.

Anticipez si possible les rénovations prévues pour la prochaine décennie et effectuez-les pendant la phase de transition.

Auteur: Roman Bosetti



Décompte selon la méthode des taux de la dette fiscale nette

Environ un tiers des personnes assujetties à l'impôt font leurs comptes avec le taux de la dette fiscale nette. Nous abordons ci-après quelques détails et écueils de cette méthode de décompte, afin que vous puissiez juger si cette méthode est judicieuse pour vous ou si votre entreprise est mieux lotie avec la méthode de décompte effective.

Généralités et modifications au 01.01.2025 suite à la révision partielle

Dans la méthode des taux de la dette fiscale nette (méthode TDFN), les chiffres d'affaires bruts (chiffres d'affaires y compris la TVA) sont décomptés à chaque fois avec les taux de la dette fiscale nette (TDFN) autorisés. Les TDFN s'élèvent entre 0,1 et 6,8 % selon l'activité. Les TDFN diffèrent selon le volume de TVA déductible ou les marges habituelles du secteur d'une activité.

Lorsqu'une entreprise assujettie a plusieurs activités, l'art. 86 al. 1 OTVA permet de demander un TDFN pour chaque activité qui représente plus de 10 % du chiffre d'affaires total imposable. Jusqu'à la fin de l'année 2024, il n'était possible de décompter qu'avec deux TDFN au maximum. Pendant la période de transition en 2025, les entreprises assujetties peuvent déclarer les chiffres d'affaires avec les TDFN correspondants et vérifier à la fin de l'année 2025 si la limite de 10 % a été dépassée dans les catégories de chiffre d'affaires. Si tel n'est pas le cas, le prochain TDFN autorisé est applicable et le TDFN non nécessaire doit être supprimé.

En ce qui concerne le TDFN de manière générale, il convient également de mentionner que les prestations soumises à l'impôt sur les acquisitions, telles que les conseils juridiques depuis l'étranger, doivent être déclarées. Comme il n'existe pas de droit à la déduction de l'impôt préalable dans le cadre de la méthode TDFN, l'impôt sur les acquisitions doit être payé au taux normal, qui est actuellement de 8,1 %. Le TDFN ne s'applique donc pas ici. Pour de nombreuses prestations soumises à l'impôt sur les acquisitions, le décompte au moyen de la méthode TDFN n'est donc pas recommandé.

Si l'on passe de la méthode effective à la méthode TDFN, il faut désormais procéder à des corrections selon l'art. 79 al. 3 OTVA sur la valeur actuelle. Inversement, lors du passage de la méthode TDFN à la méthode effective, l'impôt préalable peut être remboursé conformément à l'art. 81, al. 4 OTVA. La valeur actuelle est déterminée conformément à l'art. 31, al. 3, ou à l'art. 32, al. 2, LTVA, en amortissant pour chaque année écoulée un cinquième (20 %) des biens et services mobiliers et un vingtième (5 %) des biens immobiliers.

Exemple: Un véhicule est acquis en 2023 avec la méthode effective. Le véhicule a coûté CHF 80'000.– bruts, la TVA de 7,7 % s'élevant à CHF 5'719.59. Celle-ci a été déduite dans son intégralité. Au 01.01.2026, l'entreprise passe à la méthode TDFN. La TVA de CHF 5'719.59 peut être amortie à 60 % (3×20 %) pour les années écoulées 2023, 2024 et 2025, soit un montant de CHF 3'431.75. La correction de l'impôt préalable s'élève donc à CHF 2'287.85 et doit être déclarée au T4 2025.

Dans le cas inverse (passage de la méthode TDFN à la méthode effective), aucun impôt préalable n'a été déduit, étant donné que la méthode TDFN était utilisée jusqu'à présent pour le décompte. Avec le passage à la méthode effective au 01.01.2026, l'entreprise pourrait faire valoir le même montant de CHF 2'287.85 comme impôt préalable au T1 2026.

Limites et changement de méthode de décompte

Si la méthode TDFN est appliquée et que la limite de chiffre d'affaires de CHF 5'024'000.– ou la limite fiscale de CHF 108'000.– a été dépassée au cours de trois périodes fiscales successives, il est impératif de passer à la méthode de décompte effective conformément à l'art. 81, al. 3, OTVA. Un passage volontaire de la méthode TDFN à la méthode effective est possible au bout d'un an, l'inverse n'étant possible qu'après trois périodes fiscales complètes.



Ces deux points sont régis par l'art. 37, al. 4, LTVA. De manière générale, un passage anticipé de la méthode TDFN à la méthode effective est toujours possible, conformément à l'art. 81, al. 2, OTVA, lorsqu'au moins un TDFN autorisé a été adapté. Dans la mesure où le TDFN a été modifié en raison d'une modification des taux légaux de TVA, un changement anticipé n'est pas possible.

Si vous souhaitez changer de méthode de décompte et passer de la méthode TDFN à la méthode effective ou inversement, vous devez le communiquer à l'AFC dans les 60 jours, c'est-à-dire jusqu'au 28. février, conformément à l'art. 81, al. 1, ou à l'art. 79, al. 1, OTVA. Cette demande peut également être effectuée sur le portail électronique dans les modalités de facturation.

Procédure de déclaration

En cas de transfert de valeurs patrimoniales dans le cadre de la procédure de déclaration conformément à l'art. 38 LTVA, la partie acquéreuse reprend la base de calcul des actifs et le degré d'utilisation donnant droit à la déduction de l'impôt préalable de la partie vendeuse. Si la partie vendeuse décompte la TVA avec la méthode de décompte effective et la partie acquéreuse avec la méthode TDFN, la partie acquéreuse doit procéder à des corrections conformément à l'art. 83 OTVA. Aucune correction ne doit être effectuée sur la partie des actifs repris qui n'a pas été utilisée par la partie vendeuse pour une activité ouvrant droit à l'impôt préalable. La partie acquéreuse doit toutefois prouver l'utilisation préalable de la propriété du vendeur. Si aucune preuve ne peut être apportée, le prix de vente est considéré comme base de calcul de la correction.

Exemple: Transfert d'une branche d'activité de plus de CHF 500'000.– en procédure de déclaration de l'entreprise A SA, qui établit les décomptes avec la méthode effective, à l'entreprise B Sàrl, qui établit les décomptes selon la méthode TDFN. B Sàrl n'a pas de preuve de l'utilisation antérieure de A SA. B Sàrl doit déclarer CHF 40'500.– (CHF 500'000.– x 8,1 %) comme montant négatif au chiffre 415, ce qui entraîne un ajustement fiscal de ce même montant.

Bon à savoir

Il convient d'examiner au cas par cas si la méthode TDFN est appropriée ou non pour une entreprise assujettie. Nous nous ferons un plaisir de vous aider à effectuer les vérifications nécessaires.

Auteure: Dominique Bühler

Cryptomonnaies et échange automatique de renseignements

Le Conseil fédéral a adopté le message relatif à l'approbation de l'introduction de l'échange automatique de renseignements (EAR) international sur les cryptovaleurs avec les États partenaires concernés. L'entrée en vigueur est prévue pour 2026, avec un premier échange de données en 2027.

Situation jusqu'en 2025

Jusqu'à présent, seuls les renseignements sur les actifs traditionnels sont échangés, p. ex. les avoirs et les titres auprès des banques. En revanche, aucune information sur les cryptomonnaies ou autres valeurs négociables numériquement n'est échangée pour le moment. En outre, les bourses de cryptomonnaies et les négociants en cryptomonnaies comme Coinbase ou Binance ne sont pas soumis à l'EAR.

Le Conseil fédéral a à présent décidé de mettre en œuvre le Crypto-Asset Reporting Framework (CARF) de l'OCDE, notamment en vue de lutter contre le blanchiment d'argent et d'accroître la transparence fiscale.

Situation à partir de 2025

Outre l'Union européenne, les États-Unis devraient également mettre en œuvre les dispositions du CARF. Ainsi, à partir du 1er janvier 2026, des renseignements sur les cryptomonnaies seront collectés par l'administration fiscale et échangés entre les États participants en 2027.

Ce qui est soumis à l'obligation de déclaration

L'obligation de déclaration selon le CARF concerne ce que l'on appelle les cryptovaleurs pertinentes, définies au sens large dans la norme comme des représentations numériques d'une valeur qui sont sécurisées de manière cryptographique au moyen de la technologie Distributed Ledger (DLT) ou d'une technologie comparable et rendues utilisables pour des transactions. Tout cela est défini de manière relativement large et considéré comme pertinent si la valeur peut être utilisée à des fins de paiement ou d'investissement. L'aspect déterminant ici n'est pas la classification prudentielle dans le droit des marchés financiers, mais l'utilisation économique effective.

Les cryptoactifs pertinents comprennent, entre autres, les tokens natifs, tels que le bitcoin ou l'ethereum; les stablecoins, les actifs ou droits tokenisés, les NFT (à condition qu'ils soient négociables et qu'ils aient un objectif de paiement ou d'investissement) et les autres tokens ayant un objectif de paiement ou d'investissement.

Qu'est-ce qui m'attend?

En raison du principe de la plus-value exonérée d'impôt, la vente de cryptovaleurs du patrimoine privé est en principe exonérée d'impôt. Comme c'est généralement le cas en Suisse, il existe toutefois bien entendu des exceptions, p. ex. en cas de commerce professionnel. Bien entendu, les actifs doivent être déclarés comme patrimoine dans la déclaration d'impôt annuelle.

Les autorités fiscales seront plus attentives à la question de savoir dans quelle mesure les cryptovaleurs ont été déclarées jusqu'à présent dans la déclaration d'impôt. Les contribuables doivent donc s'assurer qu'ils ont déclaré l'intégralité des cryptoactifs concernés et les revenus qui en découlent, et ce à leur juste valeur. Si ce n'était pas déjà le cas les années précédentes, cette problématique pourrait être résolue jusqu'au premier échange de données pour les périodes fiscales déjà taxées définitivement au moyen d'une autodénonciation non punissable et sans pénalités, pour autant qu'il s'agisse de la première autodénonciation.

Il convient de vérifier dans quelle mesure les anciennes cryptovaleurs ont été déclarées dans la déclaration d'impôt. Le cas échéant, il faudrait alors procéder à une adaptation/rectification.

«Big Brother is watching you» – et cela vaut désormais aussi pour les cryptovaleurs.

Auteur: Fabian Petrus



Test de la santé informatique pour les PME

La numérisation a depuis longtemps atteint tous les secteurs. Même les petites et moyennes entreprises (PME) sont aujourd'hui fortement dépendantes de systèmes informatiques opérationnels, que ce soit pour la comptabilité, la communication avec la clientèle ou la production. Parallèlement à cela, le temps, les connaissances et les ressources manquent souvent pour vérifier régulièrement la sécurité et la stabilité informatiques. C'est ici qu'intervient le test de la santé informatique (IT-Health-Check) d'OBT: un état des lieux compact et structuré de votre environnement informatique, pratique, compréhensible et réalisable en une journée seulement.

Pourquoi un test de la santé informatique est indispensable

De nombreuses PME disposent d'environnements informatiques qui se sont développés au fil du temps: des systèmes ont été progressivement complétés, des partenaires externes ont été intégrés, des processus ont été mis en place de manière historique. Cependant, il manque souvent une vision globale. Si des mesures de sécurité existent ponctuellement, celles-ci ne sont pas systématiquement vérifiées. Les sauvegardes fonctionnent au quotidien, mais les tests de restauration n'ont jamais été effectués. Les mots de passe sont gérés individuellement au lieu d'être centralisés. De telles lacunes passent souvent inaperçues, jusqu'à ce qu'un incident survienne. Un test de la santé informatique permet précisément d'éviter cela. Il vous donne des informations claires sur l'état de votre structure informatique, met en évidence les risques et classe les mesures par ordre de priorité en fonction de leur urgence et de leur impact. L'accent n'est pas mis sur des normes théoriques, mais sur **une minimisation des risques** et **une augmentation de l'efficacité axées sur la pratique** et adaptées au quotidien d'une PME.

La démarche d'OBT: structurée, efficace et transparente

Le bilan se déroule en cinq étapes clairement définies.

1. Définition des objectifs et préparation

Des objectifs et des priorités sont fixés en collaboration avec la direction, p. ex. la sécurité informatique, la stabilité, la conformité ou l'efficacité. Nous déterminons alors si les responsables informatiques internes ou des prestataires de services externes doivent participer à l'entretien. S'il n'y a pas de responsable interne, les prestataires de services informatiques externes sont activement impliqués.

2. Analyse de la situation actuelle sur place

Nos auditeurs informatiques mènent un entretien d'enquête structuré, basé sur les six thèmes de la **norme DIN SPEC 27076**:

- organisation et sensibilisation;
- gestion des identités et des autorisations;
- sauvegarde des données et restauration;
- gestion des correctifs et des changements;
- protection contre les logiciels malveillants;
- systèmes informatiques et réseaux.

Ces champs couvrent les risques les plus courants auxquels les petites entreprises sont confrontées.

3. Évaluation et statut de risque

Toutes les réponses sont évaluées selon des critères définis. Les points particulièrement importants pour la sécurité, appelés **exigences TOP**, reçoivent une pondération plus élevée. Le résultat est présenté sous forme de **statut de risque** à l'aide d'un code couleur compréhensible et saisissable en un coup d'œil. Un **graphique radar** permet de visualiser la maturité et l'équilibre de votre structure informatique dans les six domaines thématiques. Vous verrez ainsi immédiatement où il est urgent d'agir et quels sont vos points forts.

4. Rapport et recommandations d'action

Dans le rapport succinct qui suit, vous recevez un résumé précis des résultats. Il contient des propositions de mesures concrètes, classées par ordre de priorité en fonction des dépenses, des avantages et des risques. La présentation est volontairement pragmatique: vous identifiez ainsi les mesures qui peuvent être mises en œuvre immédiatement, celles qui doivent être planifiées à moyen ou long terme et celles pour lesquelles un soutien externe est utile.

La sécurité de l'information n'est pas un projet unique, mais un processus continu, qui nécessite que vous fassiez toujours preuve de vigilance.

La valeur ajoutée pour les PME

Le test de la santé informatique fournit une analyse technique, mais aussi une base de décision claire pour la direction. Vous identifiez:

- les risques informatiques qui ont actuellement le plus grand impact sur l'exploitation et les finances;
- les mesures organisationnelles et techniques qui apportent le plus grand bénéfice;
- la manière dont votre entreprise est positionnée par rapport aux normes habituelles du secteur;
- les aspects vous permettant d'obtenir des améliorations durables grâce à des investissements ciblés.

Dans l'environnement des PME, le facteur temps est particulièrement déterminant. La démarche d'OBT est donc volontairement simple: ni processus d'audit s'étalant sur plusieurs semaines,ni rapports surchargés, mais des déclarations claires et des recommandations réalisables, dans un langage que les entrepreneurs comprennent.

Les constatations typiques des bilans de santé informatiques

D'après notre expérience, des schémas similaires apparaissent régulièrement au sein des PME. Les constatations les plus fréquentes sont p. ex.:

- **Absence de directives informatiques ou directives obsolètes**: la sécurité informatique n'est souvent pas réglementée par écrit. Les mots de passe, les autorisations ou les accès en télétravail reposent sur des habitudes plutôt que sur des directives définies.
- **Sauvegardes de données non testées:** des sauvegardes existent mais n'ont jamais été vérifiées quant à la possibilité de les restaurer. En cas d'urgence, les données risquent d'être perdues ou les temps d'arrêt longs.
- **Gestion incomplète des correctifs:** les mises à jour de sécurité sont effectuées manuellement ou de manière irrégulière, ce qui laisse ouvertes des vulnérabilités connues.
- **Comptes d'utilisateurs à usage multiple:** l'absence de séparation des droits d'administrateur augmente le risque d'erreurs de manipulation ou d'abus.
- **Faible sensibilisation des collaborateurs:** le phishing, l'ingénierie sociale ou les mots de passe non sécurisés continuent d'être des portes d'entrée centrales pour les attaque
- **Absence de plans d'urgence et de redémarrage:** souvent, on ignore qui prend quelles décisions en cas de crise ou comment l'entreprise peut continuer à fonctionner.
- **Collaboration non réglementée avec des partenaires informatiques externes:** les interfaces, les responsabilités et les niveaux de service ne sont pas clairement définis.

De tels constats ne sont pas une exception, mais la règle, en particulier dans les environnements informatiques qui se sont développés. L'avantage: il est généralement possible d'y remédier à un coût raisonnable lorsque les responsabilités sont claires et les processus définis.

Recommandations générales pour une amélioration durable

1. **Définir clairement les responsabilités:** vous désignez une personne responsable de l'organisation informatique et de la sécurité de l'information, en interne ou en externe.
2. **Promouvoir la prise de conscience:** vous organisez des formations régulières ou de courtes sessions de sensibilisation pour les collaborateurs. Les petites mesures ont de grands effets.
3. **Automatiser et tester les sauvegardes:** vous vérifiez au moins deux fois par an la restauration de vos données, et pas seulement l'existence de la sauvegarde.
4. **Assurer l'actualité du système:** vous maintenez toujours à jour les systèmes d'exploitation, les logiciels et les solutions de sécurité.
5. **Vérifier régulièrement les droits d'accès:** qui a accès à quoi? Une simple matrice des droits peut apporter beaucoup de clarté.
6. **Simuler la planification d'urgence:** vous définissez des procédures et des responsabilités claires en cas de panne informatique, de cyberattaque ou de perte de données.
7. **Gérer la documentation:** vous documentez votre environnement informatique afin de pouvoir retracer à tout moment les dépendances et les risques.
8. **Répéter le test de la santé:** vous réitérez le bilan régulièrement, en particulier après des changements organisationnels ou techniques.

Ces recommandations constituent le cœur d'une gouvernance informatique durable, quelle que soit la taille de l'entreprise ou son secteur d'activité. Elles créent de la transparence, augmentent la sécurité d'exploitation et renforcent la confiance des clients, des partenaires et des organes de surveillance.

Conclusion

Clarté, sécurité et orientation
Un test de la santé informatique n'est pas une fin en soi, mais un instrument de contrôle efficace. Il montre où vous en êtes aujourd'hui et crée la base pour des améliorations ciblées, étape par étape et sans surcharger les ressources d'une PME.

Grâce à la combinaison de **l'expérience d'OBT en matière de révision et de gestion informatique et de** la **norme DIN SPEC 27076** en tant que ligne directrice méthodologique, vous disposez d'un outil pratique pour assurer votre stabilité numérique.

Cela permet aux entrepreneurs de travailler **dans et pour l'entreprise** avec une structure informatique qui fonctionne, protège et évolue avec elle.

Auteur: Andreas Kümpel und Kilian Vogt



Guide d'autogestion pour PME

Fixer des priorités dans le quotidien des PME: voici comment les entrepreneurs distinguent ce qui est important de ce qui ne l'est pas

La multiplicité et la diversité des tâches qui font le quotidien des petites et moyennes entreprises (PME) rendent la hiérarchisation indispensable pour les entrepreneurs. Quelles sont les activités qu'ils doivent effectuer eux-mêmes et celles qu'ils peuvent déléguer? Notre guide d'autogestion fournit des réponses à ces questions.

Le quotidien des entrepreneurs est à la fois varié et exigeant: diriger des collaborateurs, négocier avec les parties prenantes, assurer le développement stratégique et financier, promouvoir les ventes. Et chaque jour, de nombreuses autres tâches les attendent. Dans les PME, il arrive souvent que les directeurs soient également propriétaires et cumulent ainsi différents rôles. C'est précisément cette diversité qui montre la pertinence de la hiérarchisation. Mais si la hiérarchisation des tâches en suspens est une tâche essentielle, elle est aussi complexe. Une approche pratique pour y parvenir est l'analyse ABC: les tâches A sont indispensables, les tâches B sont importantes, les tâches C sont moins pertinentes. Connaissez-vous vos tâches ABC? Quelle est la part de votre temps que vous consacrez aux tâches A, B et C?

Des créneaux horaires fixes pour les tâches stratégiques

Dans de nombreuses PME, on observe en outre que les tâches urgentes supplantent souvent les tâches importantes à long terme et que le quotidien opérationnel prend tellement de place que les réflexions stratégiques pour l'avenir sont négligées. Cela vaut donc la peine de réserver des plages horaires fixes dans le calendrier pour ces activités d'importance stratégique.

Lorsqu'il s'agit de l'importance des tâches, de nombreux directeurs d'entreprises en croissance souhaitent travailler davantage pour l'entreprise que dans l'entreprise. Le développement futur de l'entreprise et la réflexion sur les bonnes choses à faire sont au cœur de cette démarche.

De précieuses listes de choses à ne pas faire

Si l'on connaît ses tâches principales, il est plus facile de dire «non» et de remplir sa liste de choses à ne pas faire. Ces tâches peuvent toutefois être déléguées si elles sont pertinentes pour l'entreprise et si des capacités internes sont disponibles. Les collaborateurs prennent ainsi des responsabilités, se développent et se sentent valorisés.

Basées sur le livre éponyme de Jan Roy Edlun, les connaissances du «Monkey Management», aussi appelé théorie des singes en management, offrent ici une aide supplémentaire: les collaborateurs se rendent au bureau et souhaitent se débarrasser de leurs problèmes (un «singe» sur leurs épaules). Le risque est que ces tâches sautent alors sur vos épaules. Demandez donc plutôt à vos collaborateurs de vous proposer des solutions. En plus de vous faire gagner du temps, cela augmente aussi l'estime que vous portez à vos collaborateurs, car leur avis est pris au sérieux.

Guide d'autogestion complet pour PME

obt.ch/selbstfuehrung

Auteurs: Christoph Brunner, Thomas Züger et Alexander Fust

L'IA dans les logiciels de gestion: l'exemple d'Abacus

Depuis plus de 38 ans déjà, OBT est partenaire de distribution du logiciel de gestion Abacus. Durant cette période, beaucoup de choses se sont passées en matière de développement, et nous traversons à présent un nouveau grand processus de changement qui va fortement modifier notre manière de travailler.

Depuis longtemps, l'intelligence artificielle (IA) n'est plus une simple promesse d'avenir ni un slogan. Elle est devenue une réalité, y compris dans le domaine des logiciels de gestion. Depuis la version 2025 d'Abacus, l'IA est fermement intégrée dans la solution ERP. Elle aide à la saisie des données, mais aussi à l'analyse, au traitement et à la gestion de processus commerciaux. L'article suivant vous montre ce que cela signifie pour votre entreprise et comment vous pouvez profiter de cette évolution.

Une nouvelle génération de logiciels de gestion

Depuis des décennies, les systèmes ERP servent d'épine dorsale aux processus d'entreprise. Ils saisissent des données, gèrent des processus, assurent la transparence et augmentent l'efficacité d'une entreprise. Avec l'intégration de l'IA, l'accent se déplace de la collecte de données classique vers un logiciel qui comprend le langage, les intentions et les contextes. Abacus a franchi cette étape en lançant Abacus Intelligence. L'IA est directement intégrée dans le logiciel de gestion et réagit aux saisies vocales naturelles. L'interaction avec le logiciel est ainsi plus simple et plus directe: le système comprend ce que l'on veut dire et met en œuvre l'action souhaitée de manière autonome. «Abacus Intelligence n'est pas un simple outil supplémentaire, ce logiciel est devenu une partie du travail quotidien», explique Alexander Vegh, Chief Artificial Intelligence Officer (CAIO) chez Abacus. «Il aide à simplifier les tâches de routine et à rendre les processus à la fois plus compréhensibles et plus efficaces.» Abacus lance également un signal clair en nommant un Chief AI Officer (CAIO) au sein de la direction: l'intelligence artificielle n'est pas seulement une technologie, elle fait partie de l'ADN de l'entreprise et constitue un repère stratégique pour les années à venir.

Gestion des intentions: quand le logiciel détecte des intentions

Le cœur d'Abacus Intelligence est ce que l'on appelle le moteur d'intention, l'«intent engine». Il analyse les entrées et reconnaît l'action envisagée. Ainsi, il suffira à l'avenir d'une simple instruction telle que «Comptabiliser 250 francs sur le compte matériel de bureau» pour que le système crée automatiquement le jeu d'écritures correct. Le moteur d'intention est déjà présent dans une large palette d'applications Abacus. Il est ainsi possible de signaler les absences par chat ou d'établir et de consulter des évaluations en quelques clics. L'IA apporte également son soutien lors de la rédaction ou de la traduction de textes. Cette forme d'interaction ne remplace pas les connaissances spécialisées, mais elle élargit les possibilités, p. ex. en automatisant les processus répétitifs et en déclenchant des processus ultérieurs.

Les prochaines étapes

Avec la version 2026, l'intelligence artificielle sera intégrée encore plus profondément dans le logiciel de gestion Abacus. Elle ne sera plus seulement un complément, mais fera partie du noyau fonctionnel central. Ainsi, les processus de travail ne sont pas seulement soutenus, ils sont aussi activement façonnés. Le nouvel outil DeepAnalyze en est un exemple. Il utilise l'intelligence artificielle pour générer des codes de programme et créer ainsi des évaluations individuelles ou des programmes d'analyse en quelques secondes. L'IA écrit donc le code avec lequel les données financières sont traitées, mais n'effectue pas ses propres calculs. Cette approche garantit que les résultats sont basés sur des données financières fiables et vérifiées au sein de la plateforme Abacus.

«Avec DeepAnalyze, il est possible de générer des codes de manière dynamique afin de produire des évaluations ou des rapports en fonction de la situation», explique ainsi Alexander Vegh. «L'IA ne calcule pas elle-même, mais crée les programmes qui permettent de calculer les résultats souhaités.»

Autres domaines d'application

L'intégration de l'IA sera également visible en dehors du domaine financier avec la version 2026. Par exemple, dans la gestion des commandes, il sera désormais possible de saisir, de confirmer et d'envoyer des commandes directement dans le chat, sans avoir à ouvrir le logiciel manuellement. De plus, toutes les fonctions d'IA sont également disponibles via l'application mobile AbaClik AI. AbaClik AI est un assistant performant pour les collaborateurs, qui leur permet p. ex. de saisir leurs heures de travail ou de valider des documents, tels que des frais ou des créanciers. Il est ainsi possible de déclencher des processus de travail et de saisir des informations indépendamment du lieu où l'on se trouve.

La langue comme interface

Une caractéristique particulière d'Abacus Intelligence est sa capacité à comprendre le suisse allemand.

Le modèle linguistique reconnaît différents dialectes et peut traiter des entrées dans les dialectes zurichois, bâlois ou valaisan. Il est ainsi possible, p. ex., de saisir oralement les heures de travail, y compris les indications de pauses. L'IA transforme l'entrée en une écriture exacte, sans qu'il soit nécessaire de la retravailler manuellement.

La souveraineté des données reste en Suisse

L'utilisation croissante de l'IA soulève des questions sur la protection des données. Abacus a délibérément opté pour une solution autonome: les modèles d'IA sont exploités dans le centre de données de l'entreprise au Tessin. Ainsi, toutes les données restent en Suisse et sont soumises à la loi suisse sur la protection des données. «Abacus n'utilise pas les données clients pour la formation et ne stocke pas non plus les données d'une conversation IA en dehors du système client», souligne Alexander Vegh. «Le modèle n'apprend pas à partir d'informations productives. La souveraineté des données revient entièrement au client.» Pour les entreprises qui travaillent avec des données financières et personnelles sensibles, c'est un point essentiel.

Ce que cela signifie pour vous

L'intelligence artificielle n'est pas une vision d'avenir, mais une réalité dans le logiciel de gestion Abacus. Avec la version 2026, l'intelligence artificielle fera partie intégrante du travail quotidien. Elle change la manière dont les gens interagissent avec leur système ERP. Les processus deviennent à la fois plus efficaces, plus sûrs et plus compréhensibles. Les données restent en Suisse, l'être humain au centre.

Plus d'informations sur:
abacus.ch/fr/abacus-intelligence

Glossaire pour votre travail quotidien

Intelligence artificielle (IA)

Terme générique pour les technologies qui imitent la pensée ou l'action humaine, p. ex. par l'apprentissage à partir de données, la reconnaissance des formes ou le traitement du langage.

Apprentissage automatique

Domaine de l'IA dans lequel les systèmes apprennent de manière autonome à partir de données existantes et améliorent leurs résultats au fil du temps, sans être explicitement programmés.

Apprentissage profond (Deep Learning)

Sous-domaine de l'apprentissage automatique. Il s'agit d'utiliser des réseaux neuronaux artificiels à plusieurs couches («deep») afin de reconnaître des modèles complexes dans de grandes quantités de données. L'apprentissage profond ou «deep learning» est la base des systèmes modernes de langage, d'image et d'analyse.

Grand modèle de langage (Large Language Model, LLM)

Un modèle de langage entraîné avec de grandes quantités de texte. Il comprend le langage naturel, peut répondre à des questions, formuler des textes et interpréter des tâches. Abacus utilise son propre grand modèle de langage, qui est exploité dans un centre de données suisse.

Traitement automatique des langues (Natural Language Processing, TAL)

Capacité des ordinateurs à comprendre, traiter et produire du langage naturel. Base pour la commande vocale, les chatbots et les systèmes d'assistance comme Abacus Intelligence.

Moteur d'intention (Intent Engine)

Technologie qui reconnaît l'intention («intent») de l'utilisateur à partir d'une entrée vocale et exécute l'action correspondante dans le système (p. ex. une écriture ou une consultation de données).

IA générative

Systèmes capables de générer de nouveaux contenus (p. ex. textes, images ou analyses) sur la base d'informations existantes. Cette technologie est à la base de nombreuses applications modernes d'IA.

Prompt

Entrée ou commande permettant de contrôler un système d'IA. La qualité de la réponse dépend fortement de la précision de la formulation du prompt.

Automatisation cognitive (Cognitive Automation)

L'utilisation de l'IA pour ne pas seulement répéter des processus, mais soutenir des décisions ou déclencher de manière autonome des chaînes de processus entières.

IA explicable (Explainable AI, XAI)

Approche visant à rendre les décisions de l'IA compréhensibles. Particulièrement importante dans des domaines comme les finances ou les ressources humaines, où la transparence est nécessaire.

Souveraineté des données

Principe selon lequel une entreprise sait à tout moment où sont stockées ses données et comment elles sont utilisées. En Suisse, il s'agit d'un facteur central pour les systèmes d'IA.

Auteur: Roman Grob

Maîtriser les cyberrisques: la sécurité commence par une prise de conscience

Les cyberattaques font désormais partie de notre quotidien. Il ne se passe guère de semaine sans qu'une entreprise ne soit victime de phishing, de vol de données ou de ransomware. Les méthodes d'attaque sont de plus en plus sophistiquées, les montants des dommages augmentent, et les petites ou moyennes entreprises sont elles aussi depuis longtemps dans le collimateur des hackers. Connaître les risques et les gérer de manière ciblée permet de protéger efficacement son organisation.

Du risque à la responsabilité

Cela fait longtemps que la sécurité de l'information n'est plus un sujet purement informatique. Elle concerne l'ensemble de l'organisation, de la direction aux partenaires externes en passant par les collaborateurs. Les cyberrisques comptent aujourd'hui parmi les risques commerciaux les plus importants au monde. Une attaque réussie peut en effet détruire des données, mais aussi mettre en péril la confiance, la réputation et la productivité.

Il est essentiel que les entreprises prennent leurs responsabilités: elles doivent identifier les risques, les évaluer et prendre des mesures ciblées. La question suivante est ici cruciale: quelles informations sont critiques pour les activités de l'entreprise et comment sont-elles protégées?

Les sources de danger typiques

La plupart des incidents de sécurité commencent là où l'être humain rencontre la technologie. Un clic sur un e-mail falsifié, un mot de passe peu sécurisé ou une mise à jour manquante et ça y est, la porte est ouverte. Les risques les plus fréquents sont les suivants:

- Phishing et ingénierie sociale: les hackers trompent les collaborateurs de manière ciblée afin d'obtenir des informations confidentielles ou des données d'accès.
- Ransomware: les logiciels malveillants cryptent les données et exigent une rançon, souvent avec des conséquences désastreuses.
- Perte de données due à une mauvaise configuration ou à une utilisation abusive du cloud: des données sensibles sont rendues publiques par inadvertance ou tombent entre de mauvaises mains.
- Risques liés à la chaîne d'approvisionnement: une vulnérabilité chez un prestataire de services informatiques ou un fournisseur peut paralyser des processus commerciaux entiers.

Une protection efficace commence par la compréhension de ces risques et l'établissement de priorités.

Une sécurité bien pensée

La sécurité ne résulte pas du hasard, mais de la structure. Une procédure éprouvée s'oriente autour de cinq étapes:

1. Identifier: où se situent les valeurs, quelles sont les menaces et quelle est l'ampleur du risque?
2. Protéger: mesures techniques et organisationnelles (par ex. contrôles d'accès, cryptage, formation).
3. Détecter: surveillance, alerte et consignation des événements liés à la sécurité.
4. Réagir: un processus de réponse aux incidents clairement défini qui peut être activé rapidement et de manière coordonnée.
5. Rétablir: des sauvegardes et des concepts d'urgence qui permettent de rétablir rapidement l'exploitation.

Cette procédure, connue des normes internationales comme ISO 27001 ou le NIST Cybersecurity Framework, aide à gérer les risques de manière systématique et à les améliorer en permanence.



La technologie seule ne suffit pas

De nombreuses entreprises investissent dans des pare-feux, des antivirus et la sécurité du cloud. Mais la technologie seule ne suffit pas. Le facteur de protection le plus important reste l'être humain.

En effet, un collaborateur informé est souvent le meilleur pare-feu.

Des formations régulières, des tests de phishing réalistes et des modes de signalement clairs en cas d'urgence sont décisifs pour ancrer une conscience de la sécurité dans le quotidien.

Créer de la clarté et de la culture

Les entreprises qui prennent les cyberrisques au sérieux établissent des responsabilités claires et encouragent une culture de sécurité ouverte.

Les erreurs peuvent être abordées et les incidents sont analysés au lieu d'être étouffés.

Il en résulte une organisation qui apprend de ses expériences et devient ainsi plus résiliente.

Bon à savoir

La sécurité n'est pas un état, mais un processus.

Les cyberrisques ne peuvent jamais être totalement évités, mais ils peuvent être gérés. Les entreprises qui connaissent leurs propres valeurs, prennent les risques au sérieux et sensibilisent leur personnel, créent la base d'une sécurité à long terme et instaurent la confiance auprès des clients, des partenaires et des collaborateurs.
«La sécurité de l'information n'est pas un projet, c'est une attitude.»

Auteur: Sven Durgiai

Vous trouverez tous les contenus de l'information à la clientèle du groupe OBT sur **obt.ch/kundeninformation2026**

Die OBT Gruppe

OBT AG

Basel
Steinengraben 42 | 4051 Basel
+41 61 716 40 50

Brugg
Paradiesstrasse 15 | 5200 Brugg
+41 56 462 56 66

Lachen SZ
Oberdorfstrasse 61 | 8853 Lachen SZ
+41 55 451 69 00

Luzern
Pilatusstrasse 39 | 6003 Luzern
+41 41 227 30 70

Bern (Oberwangen)
Mühlestrasse 20 | 3173 Oberwangen BE
+41 31 303 48 60

Rapperswil SG
Fischmarktplatz 9 | 8640 Rapperswil SG
+41 55 222 89 22

Schaffhausen
Rheinweg 9 | 8200 Schaffhausen
+41 52 632 01 50

Schwyz
Rubiswilstrasse 14 | 6431 Schwyz
+41 41 819 70 70

St. Gallen
Rorschacher Strasse 63 | 9004 St.Gallen
+41 71 243 34 34

Weinfelden
Bahnhofstrasse 3 | 8570 Weinfelden
+41 71 626 30 10

Zürich
Hardturmstrasse 120 | 8005 Zürich
+41 44 278 45 00

Baker Tilly OBT AG
Hardturmstrasse 120 | 8005 Zürich
+41 44 278 45 00

Budliger Treuhand AG
Waffenplatzstrasse 64 | 8002 Zürich
+41 44 289 45 45

FIGAS Autogewerbe-Treuhand der Schweiz AG
FIGAS Revision AG
Mühlestrasse 20 | 3173 Oberwangen BE
+41 31 980 40 50

LEHMANN+PARTNER Informatik AG
Pilatusstrasse 39 | 6003 Luzern
+41 41 227 30 70

OBT bakertilly SWITZERLAND budliger FIGAS IT4HR LEHMANN+PARTNER